(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 388 797 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.02.2004 Bulletin 2004/07

(51) Int Cl.[7]: **G06F 17/60**

(21) Application number: **03254927.1**

(22) Date of filing: **07.08.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **08.08.2002 US 401807 P**
11.06.2003 US 458205
29.07.2003 US 628569
29.07.2003 US 628584
29.07.2003 US 628583

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

(72) Inventors:
- **Labrou, Yannis**
  College Park, MD 20862 (US)
- **Ji, Lusheng**
  College Park, MD 20862 (US)
- **Agre, Jonathan Russell**
  College Park, MD 20862 (US)

(74) Representative: **Hitching, Peter Matthew et al**
Haseltine Lake,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(54) Methods, apparatus and framework for purchasing of goods and services

(57) A computer system (Universal Pervasive Transaction Framework, or UPTF) includes: (a) a variety of consumer devices 102, called Universal Pervasive Transaction Devices 102 (UPTD 102) that are enabled by, and can be deployed within, the UPTF framework, for initiating requests for financial transactions relating to the purchasing of goods and services by consumers (b) a merchant device 104 for making goods and services available to consumers that own and operate the consumer devices 102 at the merchant's location, (c) a security framework and associated protocols for initiating transaction requests from the consumer 102 and merchant devices 104 and deciding the validity of the requests, (d) a system architecture for processing the partial transaction requests and initiating transaction execution with financial institutions, and (e) methods for purchasing various kinds of goods and services with the devices 102, using the transactions, security framework and protocols.

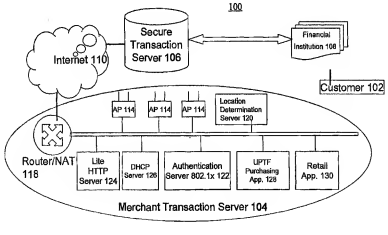


Figure 1

EP 1 388 797 A2

Description

[0001] The present invention relates generally to the fields of financial transactions, security and methods for purchasing goods and services, and a framework thereof. More particularly, the present invention relates to a computer-implemented system, methods and processes, and a framework enabling consumers to purchase goods and services, primarily at the locations where the goods and services are offered, more securely, faster and more efficiently than current methods.

[0002] To date, E-commerce (electronic commerce) for consumers (or business-to-consumer, B2C, transactions) is essentially a personal computer-mediated process. The typical consumer that wants to purchase a good or service though an e-commerce transaction ("buying on the web") has to go through the following steps:

[0003] Buy or own a personal computer (PC);

[0004] Be physically present at the computer;

[0005] Have network access;

[0006] Turn on the computer;

[0007] Log on to the computer and/or to the network;

[0008] Open a web browser;

[0009] Identify, find and visit the particular website that offers the good or service of interest;

[0010] Find the correct item or service on that website and then add it to a "shopping cart";

[0011] Provide the identity information, which might include signing up or creating an account for doing transactions in the particular website;

[0012] Enter payment and shipping information (typically a credit card);

[0013] Receive a proof of purchase for her records; and

[0014] Wait for the goods to be physically shipped.

[0015] Assuming the existence of a PC and a network connection, the remainder of the process typically requires 15-20 minutes for an experienced user. The current means and methods for consumer e-commerce transactions are expensive in terms of both money and time, complex, require proximity to a computer terminal, and are only available to a small percentage of consumers with the appropriate levels of experience and technological comfort.

[0016] Further, consumer e-commerce is basically a mail order system that replicates the "bricks and mortar" presence of a business in the virtual world and does not take advantage of merchants' "bricks and mortar" infrastructure and investment. The current system is particularly vulnerable to fraud since the vast majority of purchases on the web are CNP (Card Not Present) transactions meaning that there is no identity confirmation for these transactions, resulting in fraud costs that are primarily incurred by the merchants.

[0017] Participating in e-commerce requires a computer-literate end-user and substantial hardware. PC penetration is still very low, especially beyond the "first world" and it is unlikely that a computer-literate user and the "a PC at every household in the world" vision will happen in the next few years. A PC is a general purpose device that can be used for many different tasks, including the task of conducting e-commerce transactions. On the software side, a web browser, the universal client for electronic commerce, is not special purpose software but a client for accessing all kinds of web-based services.

[0018] Although mobile phones and PDA's can be also used for e-commerce, both follow the same paradigm, essentially bringing the browsing experience to a different device. But the essential elements of the paradigm remain, namely e-commerce is one of the multitudes of functions that can be accessed through a web browser (a universal user interface to the web) and a certain degree of computer literacy is still required, along with a considerable personal financial investment for such a client device.

[0019] In addition, various other devices including cell phones and personal digital assistants (PDAs) provide e-commerce capabilities.

[0020] Cell phones are intended for voice communication and despite the enormous success of data messaging (e. g., SMS messaging) attempts to broaden their usage by promoting them as web-browsing clients have failed. Additionally, the slow deployment and adoption of 2.5G and 3G equipment and services creates an uncertainty about the future of diversifying the usage of a mobile phone. Still, the penetration rate of mobile phones is very high.

[0021] PDA's on the other hand, have a low penetration rate and are relatively complex for use by the average person; they remain pretty much the domain of technically savvy users who carry a variety of similar gadgets. Also, their primary function is that of a personal organizer. Even though they have evolved to become very small factor personal computers, the limitations of keyboard and screen size make them inadequate at that. Special protocols such as WAP have been developed to overcome some of these types of limitations, but it has not been widely adopted, and this is not the appropriate delivery mechanism for many consumer services.

[0022] Another device of interest is the BLACKBERRY RIM and devices similar to it. The evolution of BLACKBERRY is from a pager/e-mail client device towards a full blown PDA. BLACKBERRIES are much like PDA's with anywhere wireless connectivity, as opposed to connectivity to location-specific service spots.

[0023] Smartcards are being deployed as a replacement for traditional credit cards. The deployment includes new smartcard readers that will replace the traditional credit card transaction terminals. Each bank that issues a credit card will issue it's own smartcard, so there is going to be a one to one replacement for existing credit cards. New smartcards will provide all the functions of existing credit cards but will also be used as identity cards so that for example one could log into a corporate network through a machine that is equipped with a smartcard reader. Also, smartcards are intended to be used as digital wallets so a user could "load" digital money (Mondex (mondex.com)) into the smartcard.

[0024] Smartcards have complex mechanisms that are used to improve security and protect the operations concerning digital money. But, it is unclear how smartcards are more secure than current credit cards. Of course they will be more resistant to counterfeiting but if stolen they can be used by another person; since most of the time a PIN is not required for using the card (e.g., for shopping at a store) and, if a PIN is required, knowledge of the PIN would suffice to use the card. Because a user carries many cards and it would be impractical to remember the PIN for each of them, a PIN is not required when using the card for purchases. A smartcard can store other data, so for example one could use a more advanced identification method in conjunction with a smartcard reader attached to a terminal, e.g., insertion of the smartcard to a terminal invokes a biometric-based authentication application that runs on the terminal (not on the device).

[0025] Related art includes devices for financial transactions (e.g., credit cards, smartcards, etc.), wireless devices that can be used for financial transactions (e.g., mobile phones, PDA's etc.), methods for the transactions, security frameworks and protocols, purchasing methods and workflows and Point of Sale systems.

[0026] The following discusses related art involving wireless devices and purchasing.

Wireless POS (Point of Sale) extensions

[0027] These are systems that effectively extend the cash register (POS). A store employee operates a small terminal that can transmit wirelessly to a base station at a store; the wireless terminal is a credit card reader, so that a consumer can check out (pay) at any location in a store, where the store employee happens to be. These systems have been criticized for being vulnerable to the security problems of the WEP protocol, which is used to provide a secure network connection between the wireless terminal and the base station terminal or POS.

Wireless Payment Processing

[0028] The systems essentially replace the merchant's regular phone line with a wireless link for the purpose of connecting to the financial institution that implements the transaction processing. Systems of this category are regular POS terminals that accepts credit cards (for swiping), like any other POS, but instead of using a regular land-line to connect to the processor of the merchant for authorizing the transaction, the use a wireless mobile phone connection for that purpose. Although this category by itself is not of such great interest, it is often combined with systems and innovations of some of the other discussed types, in order to provide a new kind of POS which is more portable and adaptable.

B2C (Business to Consumer) transactions using a mobile device

[0029] These are solutions that differ from desktop-based web browsing and shopping (B2C commerce) only in that the hardware client used is a mobile device. A PDA or a mobile phone that has wireless web access is used as a personal computer (similarly to any wired, or wireless, networked desktop or laptop with web access. Such solutions do not substantially differ from conducting e-commerce through a web-browser that accesses the general internet. What is important to note about these systems, is that when they are used for shopping the whole consumer experience and the associated steps and workflows do not differ from desktop-based shopping. Moreover, at the technical level, these systems use the same technologies used for desktop and laptops (for the purposes or shopping), or they rely on the stack of WAP-related protocols. The consumer has to enter payment information as she would in order to pay for something at any other e-commerce site on the web. Systems of this type are differentiated from systems that use mobile phones (described next) but require different workflows and infrastructure, even though the latter often use the WAP-related stack of protocols, because they attempt to speed-up and facilitate the submission of payment information by the user.

Mobile phone-based shopping

[0030] A variety of systems use mobile phones for conducting purchases at physical POS (merchants) and virtual POS (on the web). These systems use the mobile carrier's network to carry the transaction.

Single chip mobile phone

[0031] The customer uses a WAP-enabled mobile phone to make purchases from a participating merchant. The user experience is similar to browsing. Technically, the solution relies on the WAP (Wireless Application Protocol) stack of protocols, including WTLS (Wireless Transport Layer Security), which is similar to SSL (Secure Socket Layer) in intent. Such solutions employ a server-side wallet, which is typically provided by a participating banking institution. When accessing the merchant's virtual store, the user connects to the hosted virtual store (even though she might by physically in the physical store) and interacts with the virtual store in order to accomplish the purchase. This disconnect between physical and virtual store, requires some additional steps in the transaction workflow for making payment or for identifying the store to the user's device for the purposes of browsing (on the device) to the right place (URL and webpage). One of the goals of this approach is to involve all three major principals in the implemented system. The mobile phone manufacturer provides the WAP-enabled phone, the mobile carrier provided the value-add service to the user of using the mobile phone for purchases (also providing the hosted infrastructure and the server-side wallet) and the banking institution is the physical owner and processor of the server-side wallet related transactions. It is important to note that even if the merchant's server (the implementation of the merchant's virtual store) is located at (and perhaps operated by) the merchant's physical location, the transaction is carried by the mobile network.

Dual-chip mobile phone

[0032] This category describes systems similar to the previous one but these mobile phones include a second chip (alongside the SIM card), the WIM (Wireless Identity Module) which can read a plug-in WIM chip. The WIM module (with the inserted WIM chip) is essentially a wallet embedded on the client device (the mobile phone) and provides a single banking account associated with the mobile phone. This approach does not require a server-side wallet, but the remainder of the user transaction and interactions are the same as with single chip mobile phone systems. Dual-chip mobile phones are associated with the technological choice of separating SIM and WIM chip cards and the resulting business model of bank/carrier collaboration, i.e., keeping separate the payment function (via the WIM card controlled by the bank) and the network function (via the SIM card controlled by the network operator).

Dual-slot mobile phone

[0033] Such a system requires a phone that is equipped with a chip and slot for reading a smartcard (or even magnetic strip) based bankcard. The user inserts the card on the phone to authorize transactions using the PIN of the specific card. Such systems use protocols and technologies of mobile phones. The user of course needs to carry the actual credit cards. These systems do not require a server-side wallet in the typical sense. The server-side wallet serves as a temporary repository of the transaction data, prior to execution, but no permanent store of user's account data (or registration of accounts) is required.

Mobile phone as consumer identifier

[0034] In these systems, the mobile phone may not be essential to the transaction. When used for virtual POS transactions (B2C purchasing on the internet) the mobile phone is "reduced" to the mobile's number which is in turn used to uniquely identify the consumer at the participating merchant's site. The remaining part of the transaction might continue without involving the mobile phone, or a callback to the user's mobile phone might be required, followed by the user entering some form of confirmation, such as PIN.

Mobile phone for physical POS

[0035] The mobile phone is used partially as a consumer identifier but is essential to the execution of the transaction at a physical POS. Although implementations differ in their workflows, the mobile phone's owner will receive a transaction (some times sent as a SMS) for a physical POS transaction initiated by the merchant, which the consumer will have to authorize by entering a PIN that authorizes processing of the payment at a server-side wallet account. Confirmations (in the form of SMS messages) are sent to both mobile phone and merchant. In these systems, the initialization of the transaction is not automated but it requires the physical exchange of some account identification (e.g., phone number or some other unique ID) between merchant and consumer and keying this ID into the POS or mobile phone, along with other transaction-related information. This category can also be thought of as a sub-class of single chip mobile phone systems.

Mobile-phone shopping with direct merchant-mobile phone interaction

[0036] Systems discussed above rely on the mobile phone to carry the transaction between customer and merchant, coupled with a physical interaction (at physical POS) between merchant and consumer that exchanges an identifier (and/or associated data) that initialize the transaction. Both the merchant and the consumer use the mobile network to submit (separately) the transaction data to the carrier-operated back-end system that confirms the transaction but there is no direct electronic interaction between POS and consumer. Systems of this category on the other hand, utilize a short-range radio transport, usually wireless, so that the mobile phone can also direct connect to the merchant when the user is at the merchant's location. Such systems usually use a mobile phone equipped with Bluetooth. The transaction itself is still carried by the mobile phone network, but the Bluetooth link is used to transmit the merchant's identification code to the mobile phone, or for the mobile phone to transmit the payment receipt to the merchant.

[0037] There is another type of system that uses Bluetooth to directly interact with the POS. This is the work of the Mobile Electronic Transactions (mobiletransaction.org) consortium, whose primary members are mobile phone manufacturers. These are dual chip mobile phones with a SIM and a WIM. The WIM can be implemented in software instead of being a separate chip (e.g. a smartcard). The WIM is the (tamper-proof) certificate store and the module that is responsible for the security/transaction-related functions of the mobile phone. Bluetooth is used for a direct link with the physical POS. The phone can also be used over the GSM network for transactions on any web-accessible site. Bluetooth is used for discovery (of the POS) and for the wireless link. The WAP stack of protocols is used (WAP, WTLS, etc.) for the interaction between client (mobile) and server. Beyond that point all the workflows, security and transactions rely on using certificates. A certificate (assuming the existence of a Public Key Infrastructure, or PKI) is associated with a particular/specific banking account owned by the user; a user can have multiple certificates, each associated with a different account. Every time that the user accepts a payment, essentially she uses the certificate as a digital signature for signing the "payment contract" sent by the merchant from the physical POS that she connect to in the store. The Merchant sends that message to the acquirer, who will decrypt (with the help of the certificate authority) and then approve the payment (if all is well) and notify the merchant. The user can receive wirelessly new certificates for new accounts and at the end the user is responsible for managing the (on-the-mobile) database of certificates and the associated certification authorities. In turn the user has to understand and manage these certificates, a PKI has to be in place (including revocation of certificates for defunct accounts) and the user might need separate passwords or PIN's to unlock the certificates and or sign payment contracts with them.

[0038] It is desirable to overcome the above-mentioned, and other, problems associated with the related art.

[0039] An embodiment of a first aspect of the present invention is directed to a method for conducting a purchasing agreement for goods and services between a consumer and a merchant through a trusted a third party and using a wireless network includes generating, by the consumer, a first view of the agreement and transmitting the first view of the agreement to the third party, generating, independently by the merchant , a second view of the agreement and transmitting the second view of the agreement to the third party, and receiving, by the third party the consumer view of the agreement and the merchant view of the agreement, verifying identities of the merchant and the consumer and that the details of the independently generated views of the agreements are consistent and taking action to execute the purchasing agreement if the conditions are satisfied. The third party includes a Secure Transaction Server.

[0040] An embodiment of a second aspect of the present invention is directed to a system for conducting an agreement between two parties relying on a trusted a third party includes a first party generating a first view of the agreement and transmitting the first view of the agreement to the third party, a second party independently generating a second view of the agreement and transmitting the second view of the agreement to the third party, a wireless network connecting the first party and the second party, and a wired or wireless network connecting the second party to the third party. The trusted third party, receives the first view of the agreement and the second view of the agreement, verifies conditions including that the identities of the parties that transmitted the agreements and that the independent views of the agreement are consistent with each other, and takes action to execute the agreement if the conditions are satisfied.

[0041] An embodiment of a third aspect of the present invention is directed to a computer system for conducting purchase transactions using wireless communication between a consumer and a merchant includes a consumer operated mobile device, a merchant operated device, a trusted secure transaction server (STS) device, one or more payment service devices, a wireless communication network in communication with the consumer device and the merchant device, a communication network in communication with the merchant device and the STS device, and a communication network in communication with the STS device and the payment service devices. The consumer device, merchant device and secure transaction server device are capable of executing the Secure Transaction Protocol.

[0042] Devices and methods for wireless purchasing of goods and services by consumers are disclosed.

[0043] The overall system (hereafter referred to as Universal Pervasive Transaction Framework, or UPTF) includes: (a) a variety of consumer devices 102, called Universal Pervasive Transaction Devices 102 (UPTD 102) that are enabled by, and can be deployed within, the UPTF framework, for initiating requests for financial transactions relating to

the purchasing of goods and services by consumers (b) a merchant device **104** for making goods and services available to consumers that own and operate the consumer devices 102 at the merchant's location, (c) a security framework and associated protocols for initiating transaction requests from the consumer 102 and merchant devices 104 and deciding the validity of the requests, (d) a system architecture for processing the partial transaction requests and initiating transaction execution with financial institutions, and (e) methods for purchasing various kinds of goods and services with the devices 102, using the transactions, security framework and protocols.

[0044] Examples of goods and services include physical goods, such as grocery items, clothing, books, gasoline, etc., and services such as purchasing admission to a theater, paying for a toll, paying a fine, etc.

[0045] Benefits of the present invention over existing methods include: (a) a more secure payment method over existing and currently deployed methods, such as credit cards and smartcards, thus reducing credit card fraud and minimizing merchant's risk of fraudulent transaction, (b) a faster transaction cycle thanks to minimizing the customer's interaction with physical entities of existing Point of Sale systems (POS), i.e., cashier operators and swiping devices, and transaction parallelization, (c) enhanced customer convenience thanks to the ability to use any of multiple payment methods (bank cards, credit cards, etc.) while carrying a single device 112, memorizing a single PIN, and eliminating the signature process, and (d) increased ability to process multiple customer transactions concurrently for merchants.

[0046] Business models and methods for creating revenue from the deployment of such a system of the present invention are also presented, advocating a fee-per-transaction revenue stream. Additional potential revenue streams include the manufacturing and distribution of the handheld device 112, licensing of the technology and design of the handheld device 112, manufacturing and distribution of the merchant-owned device 102, licensing of the technology and design of the merchant device 104, and providing integration services for Point of Sale systems.

[0047] These together with other aspects and advantages which will be subsequently apparent, reside in the details of construction and operation as more fully hereinafter described and claimed, reference being had to the accompanying drawings, in which:

[0048] Figure 1 shows the major components of a UPTF system of the present invention.

[0049] Figure 2 shows a Merchant Transaction Server with all of its components in the same computing device 102 which is located in the physical store.

[0050] Figure 3 shows a MTS **104** with only the Access Points and the DHCP server in the same computing device 102, in the store's physical location and the remaining MTS 104 components located in another computing device 104, located in another physical location which is accessible by the MTS 104 (local) over the internet.

[0051] Figure 4 shows the MTS 104 (remote) located in a computing device 104 that is different than that of the MTS 104 (local) but both are physically located in the same physical store location.

[0052] Figure 5 shows an example of multiple MTS **104** deployed

[0053] Figure 6 shows an example of multiple MTS 104 deployed, sharing the Access Point infrastructure, as in a hotspot deployment

[0054] Figure 7 shows the general workflow of a consumer's interaction with the merchant, through the consumer's UPTD 102.

[0055] Fig.8 shows the general workflow for a physical goods purchase (such as a Point of Sale, or POS, purchase, or paying the bill at a restaurant).

[0056] Fig. 9 shows the general workflow for a service purchase (such as buying a ticket at a movie theater and using it for admission).

[0057] Fig. 10 shows one method for Purchase Order Acquisition

[0058] Fig. 11 represents another method for Purchase Order Acquisition that includes the STS 106 in the process.

[0059] Fig. 12 represents yet another method for Purchase Order Acquisition that includes the STS 106 in the process.

[0060] Fig. 13 shows a method for Merchant Verification.

[0061] Fig. 14 shows a method for a consumer to request a transaction.

[0062] Fig. 15 shows a method for authorizing a transaction, following a request for a transaction.

[0063] Fig. 16 shows a method for a single step request and authorization of a transaction.

[0064] Fig. 17 shows a method for creating a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution).

[0065] Fig. 18 shows another method for creating a service token (to be later used for gaining access to a service using the method of Figure 28) and authorization of the associated transaction (includes the actual payment with the related financial institution).

[0066] Fig. 19 shows a method for creating a service token (to be later used for gaining access to a service.

[0067] Fig. 20 shows a method for a single step request for a transaction, creation of a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution).

[0068] Fig. 21 shows another method for a single step request for a transaction, creation of a service token (to be

later used for gaining access to a service, using the method of Figure 28) and authorization of the associated transaction (includes the actual payment with the related financial institution).

[0069] Fig. 22 shows a method for submitting, verifying and eventually consuming a previously gained (and paid for) service token

[0070] Fig. 23 shows an alternative method for creating a service token (to be later used for gaining access to a service).

[0071] Fig. 24 shows a method for a single step request for a transaction, creation of a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution).

[0072] Fig. 25 shows a method for creating a service token (to be later used for gaining access to a service

[0073] Figure 26 shows a method for a single step request for a transaction, creation of a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution), to be used for a token created with method of Figure 27.

[0074] Figure 27 shows a method for submitting, verifying and eventually consuming a previously gained (and paid for) service token), to be used for a token created with the method of Figure 26. The described method will take place as the consumer gains access to the service (e.g., entering a movie theater, similarly to giving a ticket to the usher upon entering a movie theater).

[0075] Figure 28 shows a method for submitting, verifying and eventually consuming a previously gained (and paid for) service token), to be used for a token created with the method of Figure 18, or the method of figure 21. The described method will take place as the consumer gains access to the service (e.g., entering a movie theater, similarly to giving a ticket to the usher upon entering a movie theater).

[0076] Fig. 29 shows how consumer and merchant create their messages to the STS 106 for such a pair of messages.

[0077] Figure 30 shows the Secure Transaction Server part of Fig. 29 with further detail on the matching and cross-referenced data.

[0078] Fig. 31 shows another way of how consumer and merchant create their messages to the STS 106 for such a pair of messages.

[0079] Figure 32 shows the Secure Transaction Server part of Fig. 31 with further detail on the matching and cross-referenced data.

[0080] Fig. 33 shows a preferred encoding for a UPTD 102 message, such as the messages in Figures 29 and 31.

[0081] Figures 34 to 41 provide additional detail of a content of the transaction message part of Fig. 33.

[0082] Figure 42 describes in detail an example of a physical goods purchase such as the one in Fig. 3.

[0083] Fig. 43 is a representation of the message flow between UPTD 102, MTS 104, STS 106 and financial institution (in this case an Online Payment Service), during one (of many possible) physical goods purchase.

[0084] Fig. 44 is an alternate representation of the same information as in Fig. 43. The figure represents detail of the messages exchanged during a physical goods purchase such as the one described in Fig. 8, using the Purchase Order Acquisition method of Fig. 10.

[0085] Fig. 45 is similar to Figure 43, but the Purchase Order is requested from the STS. The figure represents detail of the messages exchanged during a physical goods purchase such as the one described in Fig. 8, using the Purchase Order Acquisition method of Figure 11 or the method of Figure 12.

[0086] Fig. 46 is a representation of a UPTF business model.

[0087] Figures 47 to 50 are drawings of a special purpose device UPTD 102.

[0088] Fig. 51 shows samples UPTD 102 displays for merchant discovery and connecting to a merchant, prior to interacting with a merchant.

[0089] Fig. 52, 53, 54 shows samples UPTD 102 displays for a physical goods purchase (as in Fig. 8).

[0090] Figures 55 and 56 show samples UPTD 102 displays for a service purchase (as in Fig. 9).

[0091] Figure 57 is an example of a computer system in which the security agreement submission protocol (SAS) view is implemented.

[0092] Figure 58 shows a method of encrypting a security agreement submission protocol (SAS) view.

[0093] Figure 59 shows a method of decrypting a security agreement submission protocol (SAS) view and how the cross reference fields are matched.

[0094] Figure 60 is another example of a computer system in which the security agreement submission protocol (SAS) view is implemented.

[0095] Figure 61 illustrates how random bit padding is applied to encrypted data fields.

[0096] Figure 62 shows an example application in purchasing of goods and services.

[0097] Figure 63 illustrates how the present invention can be used to generate 3rd-party verifiable tokens.

[0098] In the drawings, like numerals refer to like parts throughout.

[0099] The present invention is directed to methods, apparatus, frameworks and systems for purchasing of goods and services. There are many aspects of the methods, apparatus, frameworks and systems for purchasing of goods

and services described herein.

[0100] The present invention presents a new concept for performing purchasing transactions in pervasive service environments, such as ordering and paying, in physical stores (physical Points Of Sale) by a consumer that uses a mobile device. The invention includes methods for purchasing, involving a consumer operating a consumer device (universal Pervasive Transaction Device) 102 (UPTD 102), a merchant operating a merchant device 104, and third party that verifies purchasing transactions. The invention also includes apparatuses, such as the consumer device 102, the merchant device 104 and a third party device that verifies purchasing transactions. The invention also includes an overall framework and a system architecture.

System architecture

[0101] The system architecture of the UPTF of the present invention is shown in Figures 1-6, reference to which is made after an overview of an embodiment of the present invention.

[0102] One embodiment of the present invention includes Universal Pervasive Transaction Devices 102 (UPTD 102s, or UPTD 102 clients), Service Spots, a Secure Transaction Server, and an online payment service (OPS).

[0103] The Service Spots include one or more Access Points (AP) that provide wireless connectivity to UPTD 102 clients, one or more Merchant Server (MS) or Merchant Transaction Server (MTS 104), and other networking servers, such as a DHCP server, 802.1x authentication server, etc.

[0104] The Merchant Server is the merchant representative and includes UPTF Purchasing application software that handles the transaction workflow and security protocols, Merchant Retail Application software, which implements the application logic of the merchant's retail applications, and the presentation server, such as a world wide web (WWW) server, which serves the merchant content to the UPTD 102 and allows the consumer (through the UPTD 102) to interact with the Merchant Retail Application for the purposes of selecting what to order and/or purchase.

[0105] The Secure Transaction Server (STS 106) is responsible for deciding which transaction requests are legitimate and passes them to the payment service of a financial institution (preferably an Online Payment Service, or OPS, but which could also be a bank, a credit card processor, etc.) for further processing.

[0106] The Online Payment Service, which is an online account service that is run by a financial institution which is an organization that can process financial transaction requests. The following explanation is provide assuming that the financial institution is an online payment account organization such as PAYPAL, but the financial institution could be a bank, financial clearinghouse, or any institution that intermediates access to the banking system.

[0107] The final function of the STS 106 included in the UPTF of the present invention is to ensure that a transaction request is securely passed to the financial institution for fulfillment.

[0108] The architecture of the UPTF of the present invention is now explained with reference to Figures 1-6.

[0109] Fig.1 shows the architecture of a UPTF computer system 100 of the present invention. One consumer device 102 (UPTD, or universal pervasive transaction device, 102) , one merchant transaction server (MTS (merchant transaction server) 104, or simply merchant server, MS) 104, a Secure Transaction server 106 and one financial institution 108 are shown in Figure 1. The mentioned MTS 104 components represent software functionality that is delivered by corresponding software modules. The software modules included in the MTS 104 can be located in different physical locations and computer systems.

[0110] As shown in Figure 1, the UPTD 102 communicates directly with the MTS 104. The MTS 104 is coupled to the STS 106 through a network such as the Internet 110. The STS 106 then communicates with the financial institution 108 over a computer network.

[0111] Referring again to Figure 1, the MTS 104 includes access points 114, coupled to a network 116 in communication with Router/NAT 118. The MTS 104 also optionally includes a location determination server 120 and optionally includes an authentication server 802.1x 122.

[0112] Also included in the MTS 104 are Lite HTTP Server 124, DHCP Server 126, UPTF Purchasing Application 128, and Retail Application 130.

[0113] In the MTS 104, Router/NAT 118, location determination server 120, and authentication server 802.1x 122 are optional components of the MTS 104.

[0114] Figure 2 shows a Merchant Transaction Server 104 with all of its components in the same computing device 104 (optional components are omitted for brevity); the computing device 104 is located in the physical store 132.

[0115] Figure 3 shows a MTS 104 with only the Access Points and the DHCP server in the same computing device 104 (a local Merchant Transaction Server 105), in the store's physical store 132 location and the remaining MTS 104 components located in another computing device 104 (a remote Merchant Transaction Server 136), located in another physical location 138 which is accessible by the MTS 104 (local) 105 over the internet 110.

[0116] Figure 4 shows the MTS 104 (remote) 136 is located in a computing device 102 that is different than that of the MTS 104 (local) 105 but both are physically located in the same physical store location 132 and coupled to each other through pathway 140.

[0117] Figure 5 shows multiple MTS 104 devices connected to the STS 106 and Figure 6 shows multiple MTS 104 devices deployed in the same physical area (referred to as a hotspot) that covers a large retail area (where stores are available). The merchant devices share Access Points that provide wireless access to the merchant devices, which themselves might be located in the retail area or hosted elsewhere in the network. The device that is hosting the merchant stores also provides a directory 107 of the stores that are accessible via the aforementioned Access Points.

Service Spot

[0118] A more detailed explanation of a Service Spot is now presented.

[0119] A merchant essentially sets up a service spot in order to provide wireless transaction service access for the Merchant Server (MS) and connectivity to a Secure Transaction Server (STS 106). Specifically, the service spot performs at least the following functions:

Operated by an approved merchant

[0120] Provides a list of services that can be accessed through this service spot

[0121] Optionally, provides a minimum set of default services that every service spot should provide, such as user account status and balance, execution of transactions that a user conducted off-line, etc.

[0122] A service spot includes a connection (perhaps even an intermittent one) to the Internet and a wireless extension to it (WLAN, Bluetooth, IR, Zigbee, UWB, etc.).

[0123] Although IEEE 802.11b WLAN (also known as WiFi) is presented as a wireless connection, any other wireless mechanism supporting similar function could be included n a similar fashion with any other wireless mechanism or for a device 102 that operates by physically connecting into wired networks.

The UPTD 102

[0124] Next, a description of the UPTD 102 (the device 102) is presented.

[0125] The UPTD 102 includes the following features and capabilities:

[0126] 2-way wireless communication capability (preferably IEEE 802.11b (WiFi) or 802. 11a);

[0127] Processor and RAM memory;

[0128] FLASH memory for storage that is tamper-proof and protected from unauthorized reads;

[0129] a User Interface;

[0130] an LCD, such as a touch LCD);

[0131] buttons;

[0132] a Microphone;

[0133] a biometric device 102 such as fingerprint sensor;

[0134] power provided by a battery, such as a Li-ion battery, or a small solar panel or a combination of both;

[0135] a credit card size form factor;

[0136] a small footprint operating system (OS), such as LINUX; and

[0137] device 102, or software, capable of generating timestamped random number sequences.

Secure storage

[0138] These characteristics define a feature set of a UPTD 102, and each UPTD 102 is not required to include all of the foregoing features. Such a feature set can be implemented either as a special purpose device 102 (such as the one discussed later in the embodiment), or in a personal digital assistant (PDA), or a mobile phone equipped with some form of local wireless communication (Infrared, Bluetooth, WLAN, RF-ID, visual displays, etc.) capabilities.

[0139] The UPTD 102 performs at least the following functions:

[0140] Optionally, once turned on, the device 102 requests user authentication, either by the user entering a PIN and/or through a biometric method; another authentication should be requested before authorizing any transaction;

[0141] Upon authorization the device 102 scans the airwaves for available service spots;

[0142] The device connects to a service spot

[0143] the device 102 displays to the user available services (merchants and services that the merchant offers) and the user navigates through the offered services and selects which one to interact with;

[0144] the device 102 optionally presents to the user only "authenticated" services, that is services offered by an approved and authorized merchant that have been themselves been approved and authenticated;

[0145] On-board storage for records of the last n transactions; and

[0146] In a disconnected mode, the ability to cache transactions for completion when a live connection is accessible

(service spot acts as a point of access to the network).

[0147] Figure 7 shows the general workflow 200 of a consumer's interaction with the merchant 104, through the consumer's UPTD 102.

[0148] Referring now to Figure 7, upon initializing the UPTD 102 in the pre-purchasing phase 210, the UPTD 102 performs merchant discover 212 and upon the selection of the user, the UPTD 102 connects to a particular merchant 214. Depending on the type of purchase scenario, the consumer might or might not perform the "Select what to purchase" phase (optional) 216 and proceeds with either a physical goods purchase 218 or a service purchase 220. Each of these phases 218, 220 is subsequently described. Generally, the "select what to purchase" phase 216 is applicable in situations where the consumer has to place some order (such as when ordering at a restaurant, or buying tickets at a movie theater) and is not applicable in a payment at a cash register situations (such as when paying for one's groceries) at a supermarket.

[0149] Figure 8 shows the general workflow for a physical goods purchase 218 (such as a Point of Sale, or POS, purchase, or paying the bill at a restaurant).

[0150] As shown in Fig. 8, after the start 300 of the physical goods purchase 218, merchant verification 302 or merchant verification 306 occurs either prior to or after, respectively, purchase order acquisition 304. Merchant verification 302, 306 could be completely omitted.

[0151] As shown in Fig. 8, merchant verification 302, 306 is optional in the workflow 218. Merchant Verification may appear either before 302 or after 306 the Purchase Order Acquisition 304, or might be completely omitted. Every path from Start 300 to End 314 is a valid physical goods purchase workflow 218.

[0152] Each function 300, 302, 304, 306, 308, 310, 312, and 314 in Fig. 8 represents a function in the workflow 218 that is explained in subsequent figures. Each such function may be included in multiple pathways and multiple functions for some of them (e.g., Purchase Order Acquisition 304) are included.

[0153] Fig. 9 shows the general workflow for a service purchase 220 (such as buying a ticket at a movie theater and using it for admission). The term "service purchase" refers to both the purchase of a "ticket", or similar item that represents the right to access or use a service and the subsequent surrendering of the ticket for the purpose of service usage.

[0154] The merchant verification functions 324, 328 are optional in the workflow 220. Merchant Verification may appear either before 324 or after 328 the Purchase Order Acquisition 326, but not appear both before and after, or might be completely omitted. Every path from Start 322 to End 344 is a valid service goods purchase workflow. Each function in Figure 9 represents a function in the workflow 220 that is explained in further detail in subsequent figures. Each such function may be included in multiple pathways and multiple functions for some of them (e.g., Purchase Order Acquisition 304) are included.

Transaction Flows

[0155] The transaction flows associated with the purchase of virtual goods and physical goods are now discussed in detail. Detailed accounts of the transaction flows can be found in Figures 10-28, and refer to Figure 8 for physical goods and Figure 9 for virtual goods (or services), respectively.

[0156] Before a detailed description of Figures 10-28 is presented, an overview of transactions for virtual goods and for physical goods is presented.

Transaction flow for virtual goods

[0157] This workflow describes the processing involved when the service being purchased can be represented by a service token (or "virtual" goods). Typical examples of this type of transactions include purchasing a movie ticket, a bus ticket, or paying for parking or a highway toll. The transaction occurs in phases as described in Figures 7 and 9 (in more detail).

[0158] During the pre-purchasing phase, the customer discovers the available merchant in his vicinity browses and identifies the service she wishes to purchase. The details of the latter part of this phase are highly dependent on the type of service/goods to be purchased, the vendor's catalog system implementation, and the capacity of both the service spot type and client device 102. After the customer decides what to purchase, she indicates her intention to the merchant using the merchant specific interface delivered through the MS 104. After receiving the purchase request, the merchant's MTS 104 invokes the purchasing application that runs on the UPTD (described in detail herein below) and enters the purchasing phase.

[0159] The MTS 104 communicates with the UPTD 102 by generating a transaction proposal for this new transaction, which is in the form of a formatted purchase order, and sending the proposal back to the UPTD 102.

[0160] Upon receiving the transaction proposal, the UPTD 102 generates its own view of the transaction as described herein below. This view of the transaction is sent back to the MTS 104. The MTS 104 also computes its own view of

the transaction. Both views are sent in the same secure communication session to the STS 106 for verification and authentication.

[0161] The STS 106 verifies the transaction using the matching rules specified herein below. After local verification that both parties are in good standing and of the legitimacy of the transaction, the STS 106 generates responses for both parties. If any error occurred during the verification and authentication process, an error response is generated for both parties indicating a transaction authorization failure and the corresponding reasons.

[0162] If the STS approved and eventually executed the transaction, i.e., the transfer of funds from payer (consumer) to payee (merchant), through means described herein below, the consumer's UPTD will also receive data that can be used to gain access to the service purchased or to consume such service. Figures 50 to 56, described in detail herein below, elaborate on the consumer's experience during such a service purchase and the execution of the associated workflow by his UPTD.

Transaction flows for physical goods

[0163] The processing functions for transactions involving physical goods exchange are similar to those involving "virtual" goods. The most typical examples are paying for grocery, paying for appliances, etc, situations that generally describe payment at a cashier. The transaction occurs in phases as described in Figures 7 and 8 (in more detail).

[0164] A difference between transactions with physical goods and those without is the association between the goods and the consumer device 102. The problem does not appear in the case of a transaction to purchase a service, because the consumer can select the service to be purchased from his device. In the familiar example of paying for groceries using a charge card, checkout starts when a cashier opens a new virtual shopping cart on his cash register system for the new customer, then adding items to this shopping cart by scanning the items this customer wishes to purchase. Scanned physical goods are then packaged for customer pickup. After the creation of this virtual shopping cart, the cart needs to be associated with the customer's charge account. Such association is created when the customer swipes his/her credit/debit/membership card. The association can be created at any time after the virtual shopping cart is created. After the cashier finishes scanning all goods, and only after the association is created, the cashier will proceed with checkout payment by presenting the transaction to the customer charge card issuer for authorization.

[0165] The procedure is similar for using the UPTD 102. However, since the UPTD 102 communicates with the merchant MTS 104 via wireless link instead of a card swiping reader for charge card, there is a possibility of goods not being associated with the right UPTD 102. All the UPTD 102's in the range of the check-out point may be identified and potentially associated with the goods being scanned. Additional mechanisms are provided to prevent the MTS 104 from associating goods with devices 102 other than the customer's. The following is a discussion about a number of methods for creating such an association correctly.

[0166] The first option is to provide a transaction identification number to the consumer and the merchant devices. At some point prior to the handing over of physical goods, the merchant asks the consumer to present the transaction identification number and if they match, then the goods are handed over. A second option is to include a barcode or a barcode display on the client's UPTD device 102. Barcode is the simplest form of digitally readable identifier and it is almost universally available. Chances are that if a store sells physical goods, it has a barcode system installed for inventory and price check. Given the wide availability of barcode reading system and the maturity of the technology, adding a barcode to the UPTD 102 is the cheapest method to create the association because it does not require any additional hardware installation and maintenance. Also it is among the most reliable methods as well. Using this method, during the checkout process, the cashier may scan the UPTD 102 in order to receive the device 102 ID of the UPTD 102 and create the association between the goods being scanned and the customer's universal pervasive transaction account. Although the client would need to offer the UPTD 102 for scanning, the added action will increase client involvement of the checkout process and reduce the "disconnected-ness" or "not knowing what is going on" feelings of the customer. In addition, scanning of a customer's membership card is a common and well accepted practice in membership-ed retail stores so the level of added inconvenience is kept at minimum. In addition, adding a barcode reader adds security to the UPTD 102. Even though the device 102 ID of the UPTD is public and is "faked", the transaction will not succeed because of the encryption mechanism used by the STP. The barcode may be generated and displayed on the consumer device.

[0167] Other methods focus on the "physical proximity" between the client device 102 and the cashier. These methods include using technologies such as Infra Red (IR) or RF ID. In the first case, an IR transmitter is installed on each UPTD 102 and an IR reader is installed at each checkout lane. During checkout, the client needs to line up the IR transmitter with IR reader so the MTS 104 can receive the device 102 ID of the UPTD 102 over the IR communication link. In the second case, an RF ID is installed on each UPTD 102. If the ID is passive, an RF ID reader that uses an RF energy beam to activate the RF ID is required at each checkout lane. Because typically an RF ID has a very small transmission range, it is unlikely that the RF ID reader will pickup an RF ID of a device 102 in neighboring lanes or a different device 102 in the current checkout lane.

[0168] Other location determination technologies may also be employed for detecting the closest client device 102 from a cashier. Many of these techniques can use the WLAN communication on the devices 102 to perform location determination of the correct client. For example, special checkout lane antennas which can only receive wireless network signals of the client device 102 physically at the checkout counter may be installed to achieve the same level of proximity detection. The proximity of the client's device 102 can also be used as a form of security effectively preventing remote users from easily pretending to be present at a checkout station.

[0169] The UPTD 102 permits unmanned self-checkout stations, where the customer can, for example drop the items in a basket-like apparatus, so that the items can be immediately identified (perhaps using RF ID's attached to the item) and immediately generate a virtual shopping cart associated with the customer's UPTD 102 for transaction completion.

[0170] No matter what method is used to create the association, balance is struck between the probability of erroneous associations, the cost of installing and maintaining additional equipments and the convenience and ease of using UPTD 102 for checkout. At the beginning of the next phase, the transaction proposal by the merchant will include a list of items and their prices. Thus before hitting the "pay" button on his device 102, the client still has a chance to conduct a final inspection on the goods he/she is paying for.

[0171] The pre-authorization phase is identical to the transactions for virtual goods so the details are omitted here. The last "payment" phase is even simpler than that of a virtual good transaction because no token and token certificate is generated. Finally, the association between the shopping cart and the UPTD 102 can occur before or after the items are entered into the cart.

[0172] In another approach to the problem discussed, the consumer can use their device to "browse" to the virtual location of the cashier station that he is using to check out. This way he will see on his device the total amount of his purchase once the cashier has completed the "virtual" shopping cart and select to pay for it with their device. Although some other consumer might be able to do that too, one would not want to pay for someone else's groceries, so barring impatient consumers waiting in line, each consumer will end up paying for the items he is purchasing.

[0173] At a high level, the payment phase for a physical goods purchase does not differ from that of a service purchase, although in the case of a physical goods purchase the consumer does not need to present additional data in order to take possession of the purchased goods.

Returns, cancelled orders and aborted transactions

[0174] The fund transfer does not occur until the STS 106 receives acknowledgements from both client and merchant. Before this occurs, both the client and the merchant can cancel or abort the transaction at any point. Following the acknowledgement, returns are treated as a new transaction. The return transaction can also be realized in this framework, but details are omitted as it should be possible to implement such a system given the following discussion..

Details of transaction flows

[0175] Figures 10-28 are detailed descriptions of the functions shown in the purchase workflows 218, 220 of Figure 8 and Figure 9 respectively. Figures 10-28 show the actions of each of the Consumer (using UPTD 102), Merchant (using the Merchant Transaction Server 104) and Secure Transaction Server (STS) 106, and their respective communication (messages and other information exchanged between the involved parties) during the performance of the described workflow (or element).

[0176] "Consumer" stands for either the consumer's device 102 (consumer UPTF client device 102, or UPTD 102), or the combination of the UPTD 102 and its registered owner's (consumer, the person) interaction with it. The functionality of the UPTD 102 can be included in a standalone device or as part of a mobile phone or personal digital assistant (PDA).

[0177] Similarly, "Merchant" stands for either the merchant's device 104 (merchant UPTF device 104, or MTS 104), or the combination of the MTS 104 and its registered owner's (merchant, the person, or its representatives) interaction with it.

[0178] All messages from the consumer to the STS and the STS's responses to the consumer, even if such messages are forwarded to the STS by the merchant (or to the consumer, by the merchant) are encrypted according to the Security Agreement Submission (SAS) protocol, which is also referred to as the Secure Transaction Protocol (STP) or Secure Pervasive Transaction Protocol (SPTP) described) herein after. The SAS protocol is described in U.S. Patent Application No. 10/458,205, the contents of which are incorporated herein by reference, and, as related to the present invention, is discussed herein below with reference to Figures 57-63. The STP refers to the SAS adapted for purchase transactions as described in this invention.

[0179] Similarly, all messages from the merchant to the STS and the STS's responses to the merchant are encrypted according to the Secure Transaction Protocol (STP described) herein after. According to the STP, messages from

either the consumer or the merchant to the STS include an encrypted part that can only be decrypted by the STS, which has access to all the necessary information for deciding the key that was used by the consumer (or the message) in order to encrypt the encrypted part of the message. As a result, even if the consumer's message to the STS is delivered by the merchant to the STS, the merchant is unable to read the encrypted part of the consumer's message to the STS, or to alter it in such a way that the STS will still believe that the message originated from the consumer. Similarly, when the STS sends a response to the consumer, that message to the consumer contains and encrypted part, that is encrypted with a key that is unique to that consumer. Only that consumer has all the information needed to reproduce that key and use it to decrypt the encrypted part of that message. Even if the STS's message to the consumer is delivered through the merchant the merchant will be unable to read or alter the encrypted part of the message in such a way that the consumer can be deceived about the response of the STS.

[0180] The following discussion with respect to Figures 10-28 applies to both a physical goods purchase 218 shown in Figure 8 and a service purchase 220 shown in Figures 9. That is, in Figures 10-28, merchant verification refers to merchant verification 302, 306, 324, and 328; purchase order acquisition refers to purchase order acquisition 304 and 326; REQuest and AUTHorization refers to REQuest and AUTHorization 308 and 330; REQuest refers to REQuest 310 and 332; and AUTHorization refers to AUTHorization 312 and 334.

[0181] Fig. 10 shows a method 350 for Purchase Order Acquisition, referred to as Direct Purchase Order Exchange. "Purchase Order Acquisition" is the process during which the merchant communicates to the consumer the Purchase Order relating to the transaction to be attempted between merchant and consumer. A Purchase Order includes at a minimum, the amount of the transaction and some information that identifies (or can be used to identify) the merchant; in addition a Purchase Order may also include the time that the Purchase Order was issued (typically, the current local time for the merchant).

[0182] As shown in Figure 10, the consumer 102 requests a purchase order from the merchant 104 by GeneratePurchaseOrder. The merchant 104 generates a purchase order for a transaction proposal and returns it to the consumer 102.

[0183] Fig. 11 shows another method 352 for Purchase Order Acquisition, Purchase Order Request, that includes the STS 106 in the process. As shown in Figure 11, the consumer 102 requests a purchase order from a merchant 104. The merchant 104 generates a purchase order for a transaction proposal and forwards it to the STS 106. The STS 106 verifies the merchant 104 and prepares the transaction proposal for the consumer 102 using the merchant 102 purchase order (which is encrypted with the consumer's key). The merchant 104 forwards the STS 106's transaction proposal to the consumer 102. The consumer 102 verifies the STS 106's transaction proposal.

[0184] Fig. 12 shows yet another method 354 for Purchase Order Acquisition, Purchase Order Request from STS 106, that includes the STS 106 in the process. As shown in Figure 12, the consumer 102 requests a purchase order from a merchant 104 and creates and includes a REQuest PO message to the STS 106 in which SUCCess and FAILure codes in its content. The merchant 104 generates a purchase order for a transaction proposal and forwards it to the STS 106. The STS 106 verifies the merchant 104 and prepares the transaction proposal for the consumer 102 using the merchant 102 purchase order (which is encrypted with the consumer's key). The merchant 104 forwards the STS 106's transaction proposal to the consumer 102. The consumer 102 verifies the STS 106's transaction proposal.

[0185] Any of the Purchase Order Acquisition methods of Figures 10, 11, 12 can be used in each of the workflows of Figures 8,9 but each of these Purchase Order Acquisition methods has different advantages and properties. The methods of Figures 11, 12 can be used to ensure that the Purchase Order received by the consumer has been generated by the merchant that is mentioned in the Purchase Order and that this merchant is a merchant capable for transactions verified by the STS 106.

[0186] Fig. 13 shows a method 356 for Merchant Verification. As shown in Figure 13, a merchant transmits an advertisement (including the merchant legal name and address) to the consumer 102. The consumer 102 encapsulates the merchant DID and merchant advertisement in a merchant verification transaction (MVT) and transmits the MVT to the merchant 104. The merchant 104 forwards the MVT to the STS 106. The STS 106 verifies the merchant DID and the merchant legal name and address. The STS 106 provides a response (acknowledgement or failure) to the merchant 104, which forwards the STS 106 response to the consumer 102. The consumer 102 begins the transaction procedure, based upon the STS 106 response.

[0187] Fig. 14 shows a method 358 for a consumer 102 to request a transaction. This method 358 is referred to as pre-authorization because, by itself, it does not authorize a transaction to be executed with the financial institution. As shown in Figure 14, the consumer 102 generates its transaction view request and transmits its transaction view request to the merchant 104. The consumer might see on his device a representation of a Purchase Order and enter his PIN in order to initiate the process of the device creating its view request. The merchant 104 generates its transaction view request and forwards the merchant's transaction view request and the consumer's transaction view request to the STS 106. The STS 106 verifies the merchant and the consumer based upon each, respective, transaction view request, and determines whether to authorize the transaction based thereon. The STS 106 then transmits a response (an acknowledgement or a failure) to the merchant 104. The merchant 104 keeps its response from the STS 106 and

transmits the STS' response for the consumer 102 to the consumer 102. The consumer 102 then verifies the STS 106's response.

[0188] Fig. 15 shows a method 360 for authorizing a transaction (including a payment). The method 360 includes the execution of a transaction (actual payment) with the relevant financial institution. As shown in Figure 15, the consumer 102 authorizes (or confirms) a transaction by transmitting an authorization to the merchant 104. The consumer might see on his device a request to confirm and authorize this transaction, or he might see a listing of the account available for paying for this transaction and upon selecting a financial account for such payment the device will generate its authorization. The merchant 104 authorizes (or confirms) the transaction and forwards to the STS 106 its authorization and the consumer 102's authorization of the transaction. The STS 106 verifies the merchant and the consumer authorizations and determines whether to execute the transaction with the financial institution, and responds accordingly to the merchant 104 and consumer 102. The merchant 104 keeps its response from the STS 106 and transmits the STS' response for the consumer 102 to the consumer 102. The consumer 102 then verifies the STS 106's response.

[0189] Fig. 16 shows a method 362 for a single step request and authorization of a transaction. This method includes the execution of a transaction (actual payment) with the relevant financial institution. As shown in Figure 16, a consumer 102 generates its transaction view request and authorization and transmits its transaction view request and authorization to the merchant 104. The consumer might see on his device a representation of the purchase order and asked for his PIN and authorization using his default financial account for payment. The merchant 104 generates its transaction view request and authorization and forwards its transaction view request and authorization and the consumer 102's transaction view request and authorization to the STS 106. The STS 106 verifies the merchant and consumer transaction view request and authorizations, and determines whether to execute the transaction with the financial institution, and responds accordingly to the merchant 104 and the consumer 102. The merchant 104 keeps its response from the STS 106 and transmits the STS' response for the consumer 102 to the consumer 102. The consumer 102 then verifies the STS 106's response.

[0190] Fig. 17 shows a method 364 of creating a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution). As shown in Figure 17, the merchant generates a service token with timestamp and transmits it to the consumer 102. The consumer 102 authorizes (or confirms) a transaction. The consumer might see on his device a request to confirm and authorize this transaction, or he might see a listing of the account available for paying for this transaction and upon selecting a financial account for such payment the device will generate its authorization. The consumer 102 may generate a token certificate (by encrypting the token for the token's timestamp). The consumer 102 transmits the consumer's authorization to the merchant 104. The merchant 104 authorizes (or confirms) the transaction and forwards to the STS 106 its authorization and the consumer 102's authorization. In addition, the merchant 104 requests from the STS 106 a certificate for the service token. The STS 106 verifies the merchant 104 and consumer 102 authorizations and determines whether to execute the transaction with the financial institution, and responds accordingly to the merchant 104 and consumer 102. That is, the STS 106 generates a certificate for the service token encrypted with the consumer 102's key if the transaction was approved. The merchant 104 keeps its response (and stores the token certificate) from the STS 106 and transmits the STS' response for the consumer 102 to the consumer 102. The consumer 102 then verifies the STS 106's response.

[0191] Fig. 18 shows another method 363 of creating a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution). As shown in Figure 18, the consumer 102 authorizes (or confirms) a transaction. The consumer might see on his device a request to confirm and authorize this transaction, or he might see a listing of the account available for paying for this transaction and upon selecting a financial account for such payment the device will generate its authorization. The consumer 102 transmits the consumer's authorization to the merchant 104. The merchant 104 authorizes (or confirms) the transaction and forwards to the STS 106 its authorization and the consumer 102's authorization. The STS 106 verifies the merchant 104 and consumer 102 authorizations and determines whether to execute the transaction with the financial institution, and responds accordingly to the merchant 104 and consumer 102. In addition, the STS 106 generates a randomly generated number (token), to be associated with this transaction if the transaction was approved, which the STS includes to both of its responses to the merchant and the consumer. The merchant 104 keeps its response (and stores the token) from the STS 106 and transmits the STS' response for the consumer 102 to the consumer 102. The consumer 102 then verifies the STS 106's response and stores the service token.

[0192] Fig. 19 shows a method 365 of creating a service token (to be later used for gaining access to a service). As shown in Figure 19, the merchant generates a service token with timestamp and transmits it to the consumer 102. The consumer 102 acknowledges to the merchant 104 that it received the service token. The consumer 102 may generate a token certificate (by encrypting the token with a key that corresponds to the token's timestamp). The consumer 102 transmits the consumer's authorization to the merchant 104. The merchant 104 requests from the STS 106 a certificate for the service token. The STS 106 generates a certificate for the service token encrypted with the consumer 102's key if the transaction was approved. The merchant 104 stores the token certificate from the STS 106.

[0193] Fig. 20 shows a method 366 of a single step request for a transaction, creation of a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution). As shown in Figure 20, the merchant generates a service token with timestamp and transmits it to the consumer 102. The consumer 102 authorizes (or confirms) a transaction. The consumer might see on his device a representation of the purchase order and asked for his PIN and authorization using his default financial account for payment. The consumer 102 may generate a token certificate (by encrypting the token for the token's timestamp). The consumer 102 transmits the consumer's authorization to the merchant 104. The merchant 104 authorizes (or confirms) the transaction and forwards to the STS 106 its authorization and the consumer 102's authorization. In addition, the merchant 104 requests from the STS 106 a certificate for the service token. The STS 106 verifies the merchant 104 and consumer 102 authorizations and determines whether to execute the transaction with the financial institution, and responds accordingly to the merchant 104 and consumer 102. That is, the STS 106 generates a certificate for the service token encrypted with the consumer 102's key if the transaction was approved. The merchant 104 keeps its response (and stores the token certificate) from the STS 106 and transmits the STS' response for the consumer 102 to the consumer 102. The consumer 102 then verifies the STS 106's response.

[0194] Fig. 21 shows another method 367 of a single step request for a transaction, creation of a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution). As shown in Figure 18, the consumer 102 authorizes (or confirms) a transaction. The consumer might see on his device a representation of the purchase order and asked for his PIN and authorization using his default financial account for payment. The consumer 102 transmits the consumer's authorization to the merchant 104. The merchant 104 authorizes (or confirms) the transaction and forwards to the STS 106 its authorization and the consumer 102's authorization. The STS 106 verifies the merchant 104 and consumer 102 authorizations and determines whether to execute the transaction with the financial institution, and responds accordingly to the merchant 104 and consumer 102. In addition, the STS 106 generates a randomly generated number (token), to be associated with this transaction if the transaction was approved, which the STS includes to both of its responses to the merchant and the consumer. The merchant 104 keeps its response (and stores the token) from the STS 106 and transmits the STS' response for the consumer 102 to the consumer 102. The consumer 102 then verifies the STS 106's response and stores the service token.

[0195] Fig. 22 shows a method 368 of submitting, verifying and eventually consuming a previously gained (and paid for) service token. The described method will take place as the consumer gains access to the service (e.g., entering a movie theater, similarly to giving a ticket to the usher upon entering a movie theater). As shown in Figure 32, the merchant 104 requests a service token certificate for the timestamp of the STS-received token certificate. The consumer 102 generates a token certificate (by encrypting the previously received token with the key that corresponds to the timestamp of the merchant 104's request. If the certificate has been encrypted already, the consumer 102 just submits it to the merchant 104. The merchant 104 compares the token certificate with the locally -stored, previously generated (by the STS 106) token certificate for the specific consumer 102. The merchant 104 transmits a response (acknowledgement or failure) to the consumer 102, and the merchant 104 provides service to the consumer 102. This method will typically follow any of the methods described in Figures 17, 19, 20, 23.

[0196] Fig. 23 shows an alternative method 370 of creating a service token (to be later used for gaining access to a service). Unlike the method of Figures 19 the MTS 104 issues a request for a token to the STS 106 and it is the STS 106 that generates a token and its accompanying certificate.

[0197] Fig. 24 shows a method 372 of a single step request for a transaction, creation of a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution); this is similar to the method 366 shown in Fig. 20, but unlike the method 366 of Fig. 20, the MTS 104 issues a request for a token to the STS 106 and it is the STS 106 that generates a token and its accompanying certificate.

[0198] Fig. 25 shows a method 374 of creating a service token (to be later used for gaining access to a service. Unlike the methods of Fig. 17 and Fig. 18, this token creation method 374 is intended for a token certificate verification and consumption by the STS 106, such as the methods of Fig. 26 and Fig. 27.

[0199] Figure 26 shows a method 376 of a single step request for a transaction, creation of a service token (to be later used for gaining access to a service) and authorization of the associated transaction (includes the actual payment with the related financial institution), to be used for a token created with the method 374 shown in Figure 25. The method 376 shown in Figure 36 takes place as the consumer 102 gains access to the service (e.g., entering a movie theater, similarly to giving a ticket to the usher upon entering a movie theater). As shown in Figure 36, the consumer 102 generates its transaction view request and transmits same to the merchant 104. The merchant 104 generates its transaction view request and transmits its transaction view request and the consumer 102's transaction view request to the STS 106. The merchant 104 also requests from the STS 106 a service token certificate. The STS 106 verifies the merchant 104 and consumer 102 authorizations and determines whether to execute the transaction with the financial institution, and responds accordingly to the merchant 104 and consumer 102. That is, the STS 106 generates a

certificate for the service token encrypted with the consumer 102's key if the transaction was approved. The merchant 104 keeps its response (and stores the token certificate) from the STS 106 and transmits the STS' response for the consumer 102 to the consumer 102. The merchant 104 forwards the token to the consumer 102 (that is, the token and the STS response to the consumer 102 may be included in the same message). The consumer 102 then verifies the STS 106's response.

[0200] Figure 27 shows a method 378 of submitting, verifying and eventually consuming a previously gained (and paid for) service token, to be used for a token created with the method of Figure 25. The described method will take place as the consumer gains access to the service (e.g., entering a movie theater, similarly to giving a ticket to the usher upon entering a movie theater). As shown in Figure 27, the merchant 104 requests a service token certificate for the timestamp of the STS-received token certificate. The consumer 102 generates a token certificate (by encrypting the previously received token with the key that corresponds to the timestamp of the merchant 104's request. If the certificate has been encrypted already, the consumer 102 just submits it to the merchant 104. The merchant 104 forwards the token certificate to the STS 106. The STS 106 compares the token certificate with the previously-saved token certificate for the specific consumer 102. The merchant 104 receives a response (acknowledgement or failure), and the merchant 104 provides service to the consumer 102.

[0201] Figure 28 shows another method 379 for submitting, verifying and eventually consuming a previously gained (and paid for) service token. The method of Figure 28 will be typically used following the token creation methods of Figures 18 or 21. In this scenario the STS previously sent a randomly generated number to each of merchant and consumer when responding to them following a successful payment for a service by the consumer to the merchant. Upon consumption of the service the consumer need only submit to the merchant that previously obtained random number, or token, which can also be thought of a reference to a receipt.

[0202] In all of the above methods were the consumer submits a token or a token certificate to the merchant (the methods of Figures 27 and 28), this submission can be made over the wireless channel, or the token, or token certificate can be displayed on the consumer's device for the merchant or a merchant's representative to visually inspect it and compare it to the corresponding token, or token certificate, relating to the purchased transaction that the merchant has previously stored, or some representation of that token or token certificate can be displayed and read by equipment provided and/or operated by the merchant. For example, the token or token certificate can be displayed in barcode form that can be read by a barcode reader. Upon successfully reading such a barcode and comparing the read data (representing a token or token certificate) to a previously stored token or token certificate, the merchant will grant access to the consumer bearing the device that displayed the barcode.

[0203] In one embodiment, all of the messages mentioned in the previous methods (Figures 11-28) that originate either from the merchant 104, or the consumer 102 and are intended for the STS 106, are sent in pairs. Since the consumer 102 does not have a direct communication link to the STS 106, its messages to the STS 106 are submitted to the merchant 104 who then forwards them to the STS 106. Related messages intended for the STS 106 (a pair of messages, one from the merchant 104 and one from the consumer 102), represent the respective views of the merchant 104 and the consumer 102 relevant to the attempted action (e.g., requesting a transaction, authorizing a transaction, etc.). These messages are encrypted in the way described elsewhere in this document and include sufficient cross-referencing information (as described elsewhere in this document) that can be used to verify that both registered owners of the devices 102 that submit the messages are communicating the same intent to the STS 106.

Security Framework

[0204] This section discloses how the security framework and protocol for universal pervasive transactions, which is itself described elsewhere in this document, is used in this invention in order to provide security for, and guarantee certain properties of, transactions between merchants and consumers. The security framework and protocol is referred to as the Security Agreement Submission (SAS) protocol (or Secure Transmission Protocol (STP), and includes a Security Agreement Submission encryption (SASE) mechanism.

[0205] The STS 106 is the Agreement Verification Party (AVP) of the security framework and protocol for universal pervasive transactions. The merchant and the consumer are two agreement parties (AP) of the security framework and protocol for universal pervasive transactions.

[0206] The security framework delegates most of the security burden to the STS 106 and ensures that the security framework does not weaken the security functions of financial institutions and their networks. Assumptions of the security framework are that the wireless link between, for example, the consumer 102 and the merchant 104, is insecure and neither the merchant 104 nor the consumer 102 trusts one another to be whatever they claim to be and to not (willingly or unwittingly) manipulate or corrupt the transaction.

[0207] The security framework executes the following functions:

[0208] Authenticates user identity, merchant identity and transaction identity;

[0209] Ensures that transaction data (if intercepted) cannot be re-used as the transaction code is good for only one

transaction;

[0210] Ensures that no rogue party can pretend to be merchant; and

[0211] Trusts the transaction but not the parties involved.

[0212] The security framework relies on the independently created Agreement Party Views (one generated from the consumer's device 102 and one generated by the merchant 104) that together are used to uniquely identify and authorize a transaction when they both are received and processed at the STS 106, but each one of them is useless by themselves, and even if "broken" cannot be re-used. The Secure Transaction Server 106 is the intermediary server that verifies that both tokens for a transaction, one from the UPTD 102 and one from the Merchant Transaction Server (MTS 104) are valid and that they constitute a proper transaction request, before committing it to the financial institution. After confirmation of the transaction verification, a notification is sent to the UPTD 102 and MTS 104.

[0213] One difference between the security framework for UPTD 102 and other Internet-based secure transaction systems is that with the security framework described herein, there are three distinct security environments:

[0214] Between client's UPTD 102 and merchant's MTS 104;

[0215] Between the MTS 104 and STS 106; and

[0216] Between STS 106 and payment service, or financial network, or financial institution in general.

[0217] The present invention addresses the special characteristics of each component 102, 104, and 106 and connection environment involved in the whole process. Other internet transaction security frameworks such as the Secure Electronic Transaction (SET) protocol, jointly developed by VISA™ and MASTERCARD™; the Public Key Infrastructure (PKI) by VeriSign; or HTTPS/SSL by Netscape, typically assume that all parties involved in the transaction have significant computing resources. Limited by its physical dimension, battery capacity, computing power, and memory size, a UPTD 102 is not burdened with providing the platform required for such frameworks. Moreover, in terms of network connection between transaction components 102, 104, and 106, these frameworks typically abstract the connections between the components without addressing the issues specific to different types of connectivity. The purchasing environment of the present invention can employ both wireless and wired connection segments. The security settings and requirements are different in different segments and such differences are considered from the beginning of the framework's design phase.

[0218] The present invention uses the security framework and protocol for universal pervasive transactions, which focuses on providing security in the first and second types of environments, above. The third type of environment is typical for e-commerce scenarios and has been well-studied and understood, and solutions have already been proposed. Moreover, many financial institutions have established their own secure protocols for on-line transaction processing. In such an environment, in order to interact with these financial institutions, the STS 106 follows the established standards and interfaces for submitting the transactions received from service spots to these payment services after local (STS 106) processing is complete. Without getting into the details of different existing on-line transaction protocols, in the rest of this document these protocols are referred to as Transaction Over Internet (TOI) protocols.

[0219] The method of encrypting/decrypting a transaction message in the present invention, using security framework and protocol for universal pervasive transactions, is illustrated in Figures 29-41, which are explained collectively.

[0220] Figure 29 shows the secure pervasive transaction protocol encryption details 380, that is, how consumer 102 and merchant 104 create their messages to the STS 106 for such a pair of messages. The "transaction" element in each message is the content of the communicated intent (a request, an authorization, etc.).

[0221] User input refers to information entered by the consumer on the consumer device used for the purchasing transaction and by the merchant on the merchant's device. Since the merchant (person) might be busy to enter such information on a per transaction basis, the information might be permanently stored on the merchant device and read by the appropriate merchant software on a per transaction basis, instead of being entered by the merchant or his representatives. Specifically, user input refers to the PIE of the security framework and protocol for universal pervasive transactions, which in the examples of Figures 29-32 is presumed to be a PIN, but it can be any other PIE (Personal Identification Entry) in accordance to the security framework and protocol for universal pervasive transactions.

[0222] In Figures 29-32, the user input includes PIN_x and, PIN_M.

[0223] In addition, in Figures 29-32, components of messages are encrypted. These components include Transaction, UID_x, DID_M; Transaction, UID_M, DID_x.

[0224] Figure 30 shows the Secure Transaction Server 106 part of Fig. 29 with further detail on matching and cross-referenced data (which is also disclosed in further detail here in, in the discussion of the security framework and protocol for universal pervasive transactions).

[0225] Figures 31 and 32 are similar to Figures 29 and 30, respectively, one difference being that merchant 104 and consumer 102 use the Device 102 Identifier, or DID, of their interlocutor in this communication (instead of the User Identifier, or UID); this difference results in slightly different processing by the STS 106 as illustrated in Figure 41.

[0226] Figures 29-32 are explained in further detail. In Figures 29-32, the consumer 102 corresponds to the AP1 1101 shown in Figure 57, the merchant 104 corresponds to the AP2 1102 shown in Figure 57, the STS 106 corresponds to the AVP 1106 shown in Figure 57, and the encryption and decryption functions correspond to those explained with

reference to Figures 57-63.

[0227] As shown in Figure 29, the consumer 102 and the merchant 104 each separately generate and transmit to the secure transaction server 106 a message regarding the transaction. The secure transaction server 106 then decodes the separately transmitted messages and compares information included therein.

[0228] The consumer device 102 generates and transmits a consumer message (ConsumerMsg) including a plaintext part (DID_C and Time Stamp of the consumer device) and an encrypted part (Transaction view of the consumer, consumer user ID (UID_C), and merchant device ID (DID_M).

[0229] Referring again to Figure 29, the consumer device 102 generates the encrypted part of the consumer message as follows. The consumer device 102 encrypts the consumer's PIN (PIN_C) and the consumer's Random Sequence Number (RSN_C), using encoding functions (algorithms) of the Secure Agreement Submission protocol (or STP) discussed herein below with reference to Figures 57-63, to form the consumer KEY (KEY_C). The consumer device 102 then encrypts (again using the encoding functions (algorithms) discussed herein below with reference to Figures 57-63 the Transaction, consumer user ID, and merchant device ID using the consumer key, to generate the encrypted part of the consumer message.

[0230] The consumer device 102 then transmits the consumer message to the secure transaction server 106.

[0231] Likewise, the merchant device 104 generates the merchant message (MerchantMsg) using a similar procedure. The merchant message includes a plaintext part (the merchant ID (DID_M) and the time stamp of the merchant 104) and an encrypted part.

[0232] The encrypted part of the merchant message is generated by the merchant device 104 as follows. The merchant device 104 encrypts the merchant's PIN (PIN_M) and the merchant's Random Sequence Number (RSN_M), using encoding functions (algorithms) of the Secure Agreement Submission protocol (or STP) discussed herein below with reference to Figures 57-63, to form the merchant KEY (KEY_M). The merchant device 104 then encrypts (again using the encoding functions (algorithms) discussed herein below with reference to Figures 57-63 the merchant's view of the Transaction, merchant user ID (UID_M), and consumer device ID (DID_C) using the merchant key, to generate the encrypted part of the merchant message.

[0233] The merchant device 104 then transmits the merchant message to the secure transaction server 106.

[0234] Once the secure transaction server (STS) 106 receives the message (either the consumer message or the merchant message), the STS 106 decrypts each message and compares the information included in the message to the information included in the other message (either the consumer message or the merchant message).

[0235] As shown in Figures 29 and 30, the STS 106 uses the consumer's PIN (PIN_C) and the consumer's random sequence number (RSN_C), both of which are stored at the STS, to reproduce the consumer KEY (KEY_C) for the timestamp of the message using the functions (algorithms) of the Secure Agreement Submission protocol (SAS, or STP) discussed herein below. The STS 106 then uses the consumer KEY to decrypt the encrypted part of the received consumer message, again using the functions (algorithms) of the SAS (STP) discussed herein below.

[0236] Likewise, the STS 106 uses the merchant's PIN (PIN_M) and the merchant's random sequence number (RSN_M) both of which are stored at the STS, to reproduce the merchant KEY (KEY_M) using the functions (algorithms) of the Secure Agreement Submission protocol (SAS, or STP) discussed herein below. The STS 106 then uses the merchant KEY to decrypt the encrypted part of the received merchant message, again using the functions (algorithms) of the SAS (STP) discussed herein below.

[0237] Once the STS 106 has decrypted the consumer message and the merchant message, the STS 106 compares the Transaction included in the consumer message with the Transaction included in the merchant message. The STS 106 then uses local lookup (that is, lookup in a table stored in the STS 106) to determine whether the device ID (DID_M) of the merchant included in the consumer message matches (or corresponds) with the user Id (UID_M) of the merchant included in the merchant message, and whether the device Id (DID_C) of the consumer included in the merchant message matches (or corresponds) with the user id of the consumer included in the consumer message.

[0238] Figures 31 and 32 show generating, transmitting, and decoding a consumer message and a merchant message using the consumer device ID (DID_C) in place of the consumer user ID (UID_C), and the merchant device ID (DID_M) in place of the merchant user ID (UID_M). As in the case of Figures 29 and 30, the Transaction views of the consumer and the merchant included, respectively, in the consumer message and the merchant message, are compared directly with each other by the STS 106 to determine if they match. However, in Figures 31 and 32, the consumer's device id (DID_Cs) included in the consumer message and in the merchant message are compared directly with each other by the STS 106 to determine if they match, and the merchant's device id (DID_M) included in the consumer message and in the merchant message are compared directly with each other by the STS 106 to determine if they match.

[0239] Fig. 33 shows an encoding for a UPTD 102 message 400, such as the messages in Figures 30 and 32. Other variations of the encoding of a UPTD 102 message exist, for example, one that does not include either (or one of the two) of the sets of random bits before or after the "transaction message" (the content of the communication). Note, that this encoding does not elaborate on the specific format and/or representation of each of the mentioned elements. For example, a TS (a Timestamp) is actually represented based upon different encodings/representations which do

not modify/affect the workings of the protocol.

[0240] More particularly, the UPTD message 400 shown in Figure 33 is a fixed length for the entire message 400, with a fixed length for the encrypted part of the UPTD message 400. The UPTD message 400 includes a TS 404, a message type 406, DID 408, a pointer 410 to the beginning of the transaction message or length of Random 1 (414), a pointer 412 to the end of the transaction message or transaction message length of length of Random 2 (418), Random 1 (414), the transaction message 416, and Random 2 (418). The encrypted part of the UPTD message 400 includes the pointers 410, 412, Random 1 (414), the transaction message 416, and Random 2 (418). The length of each "Random" (that is, Random 1 (414) and Random 2 (418)) is random and decided at the time of message composition.

[0241] Figures 34 to 41 provide additional detail of an example of the content of the transaction message part of Fig. 33, that is the message type 406, the DID 408, and the transaction message 416 of the UPTD message 400 shown in Figure 33. Such detail is offered as an example and is drawn from the particular implementation of a UPTF system. Each one of the messages in Figures 34 to 41 corresponds to a message in one specific transaction workflow shown in Figure 43.

[0242] Figure 34 shows a REQuest for transaction by Payer (Consumer) message 420.

[0243] Figure 35 shows a REQuest for transaction by Payee (Merchant) message 422.

[0244] Figure 36 shows the STS 106's RESPONSE to REQuest for transaction by Payer message 424.

[0245] Figure 37 shows the STS 106's RESPONSE to REQuest for transaction by Payee message 426.

[0246] Figure 38 shows a Payer's AUTHorization message 428.

[0247] Figure 39 shows a Payee's AUTHorization message 430.

[0248] Figure 40 shows the STS 106's RESPONSE to AUTHorization for transaction by Payer message 432.

[0249] Figure 41 shows the STS 106's RESPONSE to AUTHorization for transaction by Payee message 434.

[0250] The following discussion is an embodiment implementing the software components on the UPTD 102, the service spot (that is, the MTS 104) and the Secure Transaction Server 106.

Software

Device 102 software

[0251] The device 102 software includes all the software that is executed on the UPTD 102. The primary functions of the UPTD 102 software include:

[0252] Identifying a service spot (104) and listing the available services in that particular location;

[0253] Enabling the user to interact with the available services;

[0254] Perform purchasing transactions; and

[0255] Interact with the user during purchasing transactions;

[0256] The above describes the minimum necessary software functions for a UPTD 102. In addition, a device 102 may provide access to device 102-stored data, such as receipts and records of past transactions, user spent organized by account, date, etc., and so on. In addition, a device 102 may provide software-supported functionality that is unrelated to supporting the authorization of financial transactions, or to financial data altogether, such as games, calendar, contacts, etc.

[0257] In addition, device 102 might require authenticating its user prior to operation (or purchasing). Upon turning on the device 102 it might requests user authentication, either through a biometric authentication (such as a fingerprint) or a device access PIN. In the case of fingerprint authorization the device 102 displays a message to the user to put their finger on the appropriate area on the device 102. If a PIN is used for authorization, a numeric keypad is displayed on the device 102. If the device 102 has a touch screen the user can enter the PIN in a fashion similar to entering a PIN at an ATM, If a conventional display is used, then the user has to navigate the keypad using the device 102's buttons (4 buttons for up-down-left-right, or 8 buttons for 8 possible directions of movement) and then press the device 102's "enter" button to accept an entry. As a convenience to the user, after each number entry, the highlighted button will be the middle button in the display (in a typical 3-3-3-1 keypad arrangement, this button will be the number 5).

[0258] After authenticating the user, the device 102 scans all channels for available access points (potential service spots 104) in the user's proximity. This process can also take place in the background while the user is going through the process of authenticating herself to the device 102. During this "discovery" phase the device 102 identifies all available service spots (multiple access points might belong to the same service spot) and receives the "homepage" for each service spot. The homepage for each service spot might be encoded in the service spot's network ID (SSID), or it might be exchanged between the device 102 and the service spot 104 using a service discovery protocol. When the list of service spots has been compiled the device 102 launches a browser window which displays a locally generated information message (e.g., HTML page) for the user to inspect. The browser window displays the names of the available service spots as a listing that describes the service spot. For example the device 102 displays one service spot per

line and no more than 4 lines per page (for readability purposes), although the font size and number of lines per screen might also be user-configurable. An example of the outcome of this stage can be seen in Figure 51.

[0259] The listing of merchants appears as follows:

[0260] Sam's Restaurant

[0261] Jeff Books

[0262] Movie Park

[0263] The user then selects which merchant they would like to interact with. The selection is done either using the touch display or by navigating the page using the device 102 arrow-keys and the enter button. The overall experience is similar to web browsing. Upon selecting a merchant to interact with, for example, Movie Park, the user sees a listing of services offered by that merchant. For example:

[0264] Buy tickets for a movie

[0265] View movie schedule

[0266] Pay at concession stand

[0267] The user selects which service she wants to interact with and she proceeds depending on the selected service in a manner similar to purchasing or transacting through a browser. When the user is ready to start the payment phase, he starts the purchasing application running on his UPTD 102. It is important to note that the user explicitly invokes this application, either by selecting it from a listing of application available on the device or by pressing a button that has been "linked" to that application. As the user, durng payment, enters his PIN it is important that the user always starts himself the purchasing applications so that he realizes that if his PIN is requested without him having started the payment application first, then most likely some untrusted party is attempting to trick the consumer into entering his PIN in some remote web page, thus attempting to steal the user's PIN. Even though obtaining the PIN is such (or anyother) manner, would not be sufficient for a fraudulent party to attempt a purchasing transaction impersonating a consumer operating a UPTD 102, forcing the user to start the purchasing application himself, through some action that involves the invocation of the proper application on his own device, further strengthens the security of the system. So. when the user reaches the point of having to approve payment, the user is requested, by the purchasing application for her PIN and then she is presented with the listing of available financial accounts (credit card, bank accounts, etc.) that she can use for this particular payment. The device 102 preferably displays alias for these accounts, as opposed to actual account numbers. For the purposes of the presented method, it is not necessary that the device 102 maintains account numbers locally, a precaution which adds to the security of the overall method. The listing of the available accounts is updated in the background as the device 102 uses the ubiquitously offered (by all service spots) "update account" service, through which the STS provides the device 102 with an up-to-date listing of device 102-associated accounts. After the user selects the account (the PIN could optionally be requested after the selection has been made, as opposed to before it), the transaction request is generated and transmitted as described previously.

[0268] The device 102 might keep a history of prior receipts, organized for viewing in multiple ways for the user's benefits. These receipts do not contain actual account numbers and they are generated from the approved transaction messages that the device 102 has received. When the user wants to gain access to a paid service, the user submits the token or token certificate that is associated with the receipt, by invoking a local, i.e., running on the UPTD, application, for example the "submit receipt" application. The reason and mechanism for this invocation are the same as those discussed previously with respect to the purchasing application.

[0269] When the user is done interacting with the service, she might select to turn the device 102 off or the device 102 might turn itself off after a fixed (or user-specified) time period. Turning the device 102 off could mean either of the following: the device 102 shuts itself off the way a personal computer does and has to be rebooted the next time, or, the device 102 goes into suspend mode where the device 102 is powered down after it has saved its memory state to a rewritable memory and upon rebooting it can restore itself by reading its prior memory state and loading it into runtime memory, or, it can go into sleep mode, meaning that it shuts down all power consumption except retaining memory and can be restored immediately by powering up essential components.

Merchant software

[0270] The merchant software includes the service spot, a connection to the STS 106 and some integration (in most cases) with the merchant's point of sale system. The primary functions of the merchant installed software are:

[0271] carry out the transaction workflow that is relevant to the type of business that the merchant is carrying out;

[0272] implement a service spot, meaning that it can display the merchant-offered services on the customer's UPTD 102;

[0273] connect securely to the STS 106 so that it can submit the relevant parts of a transaction request; and

[0274] integrate with the merchant's billing system so that appropriate pricing is displayed to each user for each prospective transaction and the necessary records for each successful transaction are created.

[0275] In cases where the merchant 104 also enables self-checkout, additional hardware and software supporting

same is included to support customer self-checkout

[0276] The core of the service spot is a wireless access point (or a set of them) which can provide access to the services that are available at the service spot. The wireless access point might support any or all of available wireless technologies, such as 801.11 b, Bluetooth, RF-ID, Zigbee, IR and so on, meaning that it can provide (wireless) access to any device 102 that supports any of these technologies. It is not necessary that the access point is wireless and indeed the same functionality could be achieved if the client device 102 engages in some form of physical contact with the access point, for example swiping a card, waving a card at very close proximity to the access point and so on. For the most part though, the benefits of the discussed apparatus and methods will be evidenced in the case of a wireless interaction between the device 102 and the access point.

[0277] One configuration included on an MTS 104 providing a service spot includes:

[0278] a laptop computer by FUJITSU LIMITED, WINDOWS XP, .NET FRAMEWORK, WLAN AP (directly connected), WEB SERVER, DHCP SERVER, NET WEB APPLICATION (STORE), a web service interface for STS 106 communication, NET application (C#) for purchasing application, and wireless communications to a UPTD 102 for purchase transaction messages.

[0279] The subsequently described method for the interaction between a service spot and a UPTD 102 is only one of many ways of implementing the functionality of displaying on the UPTD 102 the available service spot services and managing the interaction between the device 102 and the service spot.

[0280] A service spot may include multiple access points 114. The service spot provides wireless access to a web server that provides the service spot's interface to the available services and the means for interacting with them. A compatible and enabled client device 102 receives the address of the homepage of the service spot after establishing a connection to the service spot through any of the service spots' access points. In WLAN terms a service spot is identified by a SSID and the service spot's homepage might be included in the SSID itself. The homepage of the service spot provides a listing of the available services. Broadly speaking, there exist two types of services: (a) services that are local and particular to the service spot, e.g., browsing a catalog or menu, paying a bill, purchasing an item, etc., and (b) remote services that might be accessed through the service spot but are not executed by the particular service spot, e.g., providing account balances, service listing for neighboring service spots, etc. In the latter case, the service spot is only providing network connectivity between the UPTD 102 and some other service spot or other authorized system. For the purposes of establishing wireless network connections to authorized devices 102 the service spot might also run a DHCP server so that a temporary network address can be assigned to the device 102 for the duration of the interaction between device 102 and service spot.

[0281] Upon granting a UPTD 102 a connection to the service spot the service spot server acts as a web server allowing the user to browse the services. Two critical functions of the server are to manage the workflows associated with the specific transactions that the service spot offers and to authorize the service spot's end of a transaction. The first part is similar to what most e-commerce web servers do when offering purchasing services to online customers. In the service spot case though, the necessary workflows might be different, occasionally more complex and in the case of some types of transactions they might require coordination with other service spot systems (e.g., when purchasing a physical good and allowing a self-checkout). The service spot will act as a conduit for transmitting the client-generated part of a transaction request to the STS 106 and to deliver the response of the server to the client device 102. The process of transmitting the client's part of the transaction to the merchant server and the merchant server's response to the client could be implemented either as an integral part of the web-based interaction between the device 102 and the server or as a separate protocol (synchronized with the browsing). After the service spot receives an approval from the STS 106 then it can pass it to the appropriate POS component for further processing (e.g., printing a hardcopy receipt, if the user so requires).

[0282] The service spot communicates (using a secure wired network) with the STS 106. As mentioned, the service spot acts as a medium for transporting the device 102's transaction request to the transaction server. Upon processing all the constituent parts of the transaction, the transaction server generated response, if any, will be forwarded to the device 102 and the merchant respectively. This response concludes the transaction between the merchant and the customer.

[0283] The service spot will require differing degrees of POS integration that depends on the type of store and the complexity of the existing POS infrastructure. In that sense, the requirements are not different from integrating any payment/register solution, such as a credit card processing device 102 into the store IT infrastructure. An additional requirement though, is that the store makes available an electronic version of the store-offered services, similar to creating an electronic storefront (web-store).

Secure Transaction Server 106 software

[0284] The STS 106 has incoming connections from multiple service spots and outgoing connections to one or more financial institutions. The primary functions of the STS 106 are:

[0285] To process the merchant 104 and the consumer 102 parts of each transaction;

[0286] To properly decrypt and match the corresponding parts of each transaction in order to identify that the requested transaction is valid and it was properly requested by all involved parties;

[0287] To notify the requesting merchant and customer that a transaction request has been approved and authorized;

[0288] To, in parallel, or subsequently, forward the transaction request to the relevant payment service; and

[0289] To keep records of merchant and consumer accounts, UPTD 102's and their related data and to record all transactions.

[0290] To control account registration and account deactivation for lost or stolen devices.

[0291] The interaction with the financial institution 108 depends on the nature of the arrangement with the Institution 108 and the nature of the account or accounts associated with the device 102.

[0292] If the device 102 is associated with a single online payment service account (such as PayPal or C2it) the interaction with the Institution can be accessed in any of the following two ways. In the absence of an arrangement with the third party, the institution will be accessed through the web-based financial Institution's interface, which would require a web-scraping script for logging into the corresponding user account and performing the actions that a web user would perform if she accessed the account through the web, using a web client. Preferably (for purposes of robustness, speed and efficiency) the third party system will be accessed through an available Application Program Interface (API) that will offer direct access to the transaction posting system; such transactions would have to occur via a secure network connection (either in the form of a dedicated network, VPN, or through the use of appropriate security protocols, such as SSL).

[0293] If the STS 106 has to handle multiple financial accounts directly (meaning if the STS 106 is its own online payment service) then the server will have to connect to proprietary financial networks or to Automated Clearinghouse Network (ACH) and access each bank account separately in order to process each transaction request. Although such a system is significantly more complex that the one described previously, its implementation follows established technologies and has been done already by a variety of online payment services

[0294] The architecture of the STS 106 is the typical 2-tier or 3-tier one for this type of application, i.e., a database server accessed through an application server and application layer API's. Multiple servers might be deployed in order to accommodate load and fast access due to geographic constraints and heavy transaction volume.

[0295] The primary function of the server is to authorize transaction requests 106 using the STP. The server keeps a real-time and up-to-date record of all the UPTD 102's in use; specifically, the server knows the device 102 ID of each UPTD 102 in circulation, the user account associated with the device 102 and the transaction authorizing PIN issued for each device 102. The server also does the same for each merchant-owned service spot. As long as the server knows the seed for each client device 102 (and merchant service spot), corresponding PIN's, random generator and the means for resolving the time of a generated ID by the client, it will be able to decrypt the constituent parts of a transaction request and decide whether to authorize a transaction.

[0296] Beyond serving the functionality discussed, the server might provide implementation and support for additional applications, such as the cashier-less store discussed elsewhere in this document, analytics on transactional data, monitoring of customer transactions in order to provide opportunities for customized offers by financial Institutions to consumers, etc. Such applications can be designed on top of the typical 2-tier or 3-tier architecture mentioned before.

[0297] One example of an STS 106 configuration includes a DELL desktop computer, WINDOWS XP, NET FRAMEWORK, NET application, C# (for STS 106 functionality), and a web services (e.g., WSDL and SOAP-based) Interface for MTS 104 communication.

[0298] Figure 42 describes 440 in detail a physical goods purchase such as the one shown in Fig. 6. Each of Purchase Order Acquisition (Fig. 10), REQuest (Fig. 14) and AUTHorization (Fig. 15) can be seen in further detail as the actions and messages of the consumer and merchant devices and of the STS 106 are described. These actions are carried out by the purchasing applications of the UPTD 102 and the MTS 104 and by the STS 106.

[0299] As shown in Figure 42, the UPTD 102 transmits to the MTS 104 a Request PO, and the MTS 104 sends to the UPTD 102 a PO (purchase order) in response to the UPTD 102's request. The UPTD 102 displays the PO to the user, and requests that the user Input to the UPTD 102 a PIN. The UPTD 102 prepares and transmits a UPTD Encrypted REQuest to the MTS 104.

[0300] Upon receiving the UPTD Encrypted REQuest, the MTS 104 prepares an Encrypted MTS REQuest, creates an envelope (including the UPTD & MTS REQ) and transmits the envelope to the STS 106.

[0301] Upon receiving the envelope, the STS 106 decrypts the MTS REQuest, decrypts the UPTD REQuest, compares the MTS REQuest and the UPTD REQuest with each other, and, based upon the results of the comparison of the MTS REQuest and the UPTD REQuest with each other, prepares encrypted responses (such as PAYMENT START if the comparison by the STS 106 had indicated that MTS REQuest and the UPTD REQuest agree with each other) for the MTS 104 and the UPTD 102. The STS 106 includes a listing of the accounts associated with the specific UPTD 106 in its response to the UPTD 106. The STS 106 then sends the responses to the MTS 104 in a response envelope.

[0302] Upon receiving the response envelope from the STS 106, the MTS 104 opens the envelope, marks the trans-

action as PAYMENT START (if the comparison by the STS 106 had indicated that MTS REQuest and the UPTD REQuest agree with each other), and transmits to the UPTD 102 the STS 106 response included in the response envelope.

[0303] The UPTD 102 then decrypts the message from the STS 106. If the message from the STS 106 indicates that the REQuest was acceptable (that is, if the comparison by the STS 106 had indicated that MTS REQuest and the UPTD REQuest agree with each other), then the UPTD 102 queries the user for AUThorization. The UPTD 102 displays a listing of accounts received by the STS 106 and waits for the user to indicate which account to use for the purchase and authorize the transaction. If the user AUTHorizes (that is, provides AUTHorization), the UPTD prepares and forwards to the MTS 104 an encrypted AUTHorization.

[0304] The MTS 104 then prepares encrypted MTS AUTHorization, creates an envelope (including the UPTD and the MTS AUTHorizations) and transmits the envelope to the STS 106.

[0305] Upon receipt of the envelope, the STS 106 opens the envelope, and decrypts the MTS AUTHorization and decrypts the UPTD AUThorization. If both the MTS AUTHorization and the UPTD AUTHorization are acceptable to the STS 106, the STS 106 transmits to the financial institution 108 (not shown in Figure 42) in communication with the STS (such as PAYPAL) a message to execute the authorized transaction.

[0306] Upon completion of the authorized transaction, the financial institution transmits a message to the STS 106 indicating whether the transaction has succeeded. If the financial institution indicates in the message that the transaction has succeeded, the STS 106 prepares encrypted responses for the MTS 104 and the UPTD 102 and transmits the encrypted responses to the MTS 104 in a response envelope.

[0307] Upon receiving the response envelope, the MTS 104 opens the envelope, marks that transaction as PAYMENT RECEIVED, and forwards to the UPTD 102 the STS 106 response.

[0308] The UPTD 102 receives the STS 106 response.

[0309] Fig. 43 is a representation of the message flow between UPTD 102, MTS 104, STS 106 and payment service (in this case an Online Payment Service) 108, during a physical goods purchase.

[0310] Referring now to Figure 43,

[0311] 1 the UPTD 102 transmits a Request PO (purchase order) to the MTS 104;

[0312] 2 the MTS 104 sends the PO to the UPTD 102;

[0313] **3** the UPTD 102 sends a UPTD transaction REQuest to the MTS 104; user enters PIN

[0314] 4 the MTS 104 sends an MTS transaction REQ and UPTD REQ to the STS 106;

[0315] 5 STS requests from Online Payment Service the account listing for consumer

[0316] 6 STS receives Online Payment Service account listing

[0317] 7 the STS 106 sends a response to the REQs to the MTS 104;

[0318] 8 the MTS 104 forwards the STS response to REQ to the UPTD 102;

[0319] 9 the UPTD 102 sends the UPTD transaction AUTHorization to the MTS 104;

[0320] 10 the MTS 104 sends the MTS transaction AUTH and UPTD AUTH to the STS 106;

[0321] 11 the STS 106 sends the transaction to an online payment service 108

[0322] 12 the STS 106 receives the online transaction service 108 response;

[0323] 13 the STS 106 sends a response to AUTH to the MTS 104; and

[0324] 14 the MTS 104 forwards the STS 106 response to AUTH to UPTD 102.

[0325] Figure 44 is an alternate representation of the same information as in Fig. 43, and the above-mentioned functions 1-14 explained with respect to Figure 43 also apply to Figure 44.

[0326] Figure 45 is similar to Figures 43 and 44 but it represents detail of the messages exchanged during a physical goods purchase such as the one described in Fig.7, but using the Purchase Order Acquisition method of Fig. 11.

[0327] Referring now to Figure 45,

[0328] 1 the UPTD 102 sends a Request for a purchase order (Request PO) to the MTS 104;

[0329] 2 the MTS 104 sends the MTS PO to the STS 106;

[0330] 3 the STS 106 sends Transaction Proposal to the MTS 104;

[0331] 4 the MTS 104 forwards the Transaction Proposal to the UPTD 102;

[0332] 5 the UPTD 102 sends UPTD transaction REQuest to the MTS 104;

[0333] 6 the MTS 104 sends the MTS transaction REQ and UPTD REQ to the STS 106;

[0334] 7 STS requests from Online Payment Service the account listing for consumer;

[0335] 8 STS receives Online Payment Service account listing;

[0336] 9 the STS 106 sends a response to REQ to the MTS 104;

[0337] 10 the MTS 104 forwards the STS response to REQ to UPTD 102;

[0338] 11 the UPTD 102 sends UPTD transaction AUTHorization to the MTS 104;

[0339] 12 the MTS 104 sends the MTS transaction AUTH and UPTD AUTH to the STS 106;

[0340] 13 the STS 106 sends the transaction to the online payment service 108 (such as PAYPAL);

[0341] 14 the STS 106 receives the online payment service response;

[0342] 15 the STS 106 sends a response to AUTH to the MTS 104; and

[0343] 16 the MTS 104 forwards the STS response to AUTH to UPTD 102.

Business models and revenue generation

[0344] Fig. 46 is a representation of a UPTF business model 500. As shown in Figure 46, multiple customers 102 communicate with respective merchant servers 104 through wide area local area networks (WLANs) 105. The merchant servers 104 communicate with the secure transaction server 106 through the Internet 110. The secure transaction server 106 communicates also through the Internet 110 with an online payment service 108, which communicates with various financial institutions 108-1, 108-2, and 108-3. Therefore, the secure transaction server 106 may communicate with multiple online payment services 108.

[0345] In the UPTF business model 500 shown in Figure 46, merchants 104 and/or online payment services 108 and/or financial institutions 108-1, 108-2, and 108-3 are charged a fee per transaction. This fee can be a flat fee or a percentage of the total amount of the transaction, or a combination thereof, and it can be charged to any of the consumer, merchant, or financial institution.

[0346] In the presented system architecture, the Secure Transaction Server 106 is the necessary component for resolving transactions and making possible the further processing. Three parties rely on the successful processing of the Transaction Server: customer, merchant, on-line payment service. All three can be charged a fee per transaction processed, since all three parties benefit from the process.

[0347] Many types of pushed information can be supplied to the devices 102. For example the user can receive pre-approved credit cards (or special per transaction APR's, or special offers and coupons) as the user is about to make a purchase. For such mechanisms to work, real-time access to the STS 106 will be necessary enabling the deployment of such applications as add-on services to the STS 106. Parties, such a bank who issued a particular credit card, will be the paying customer in such a case.

Devices 102 in the UPTF framework

[0348] The UPTD 102 is a single device that replaces the multiple plastic credit cards and smartcards that everyone typically carries on their person and provides a more convenient, efficient and secure way to conduct a credit card purchase. Through a wireless communication capability built into the device 102, a transaction can be conducted without the placement of the card into a card reader or a user signature. This leads to reduced time and labor for every purchase, benefiting both consumer and merchant. A Secure Transaction Service (STS 106) is defined that will verify each transaction prior to being committed, providing protection against fraud.

[0349] The main features of the device 102 are:

[0350] Wireless 2-way communication; and

[0351] Limited, simple user interface, consisting of a display (e.g., LCD) and several buttons for an on/off switch, navigation and confirm/pay/transact functions.

[0352] Mobile phones with 2-way wireless communication, such as IR, Bluetooth, WLAN, etc, PDA's with 2-way wireless communication, such as IR, Bluetooth, WLAN, etc, and special purpose devices described next can be used as consumer devices in the described invention.

[0353] Figures 47 to 50 show one particular embodiment of a UPTD 102; this is a new device, whose only purpose is to perform purchasing transactions in the way described in the current invention. Examples of other devices which may execute UPTD 102 functions include mobile phones or personal digital assistants (PDAs).

[0354] Referring now to Figure 47, this UPTD 102 includes a liquid crystal display 502 and buttons 504 on the front side, and a fingerprint sensor 506 and a battery access screw 508 on the back side. The dimensions of the UPTD 102 are 54 mm by 85.6 mm.

[0355] Figure 48 shows a credit card-sized processor board 510, a compact flash WIFI card 512, and a compact flash connector 514 included on the UPTD 102. The compact flash 512 may be extended on a WLAN card beyond the credit card board 510 to accommodate an antenna.

[0356] Figure 49 shows a side view of the UPTD 102. The height of the UPTD 102 is approximately 20 mm. The side view of the UPTD 102 shows the relative positions of the buttons 504, the LCD 502, the compact flash 512, the credit card board 510, the fingerprint sensor 506 and the battery 516.

[0357] Figure 50 shows an alternate side view of the UPTD 102. The height of the UPTF 102 is approximately 20 mm. The side view of the UPTD 102 shows the relative positions of the buttons 504, the LCD 502, the compact flash 512, the credit card board 510, the fingerprint sensor 506 and the battery 516.

[0358] The discussed UPTD 102 is one of the devices that are enabled by and can be deployed within the UPTF framework of the present invention.

[0359] The complete UPTD 102 includes a fingerprint sensor, WLAN (or other wireless communication), display, and other features as discussed herein above. The UPTD 102 is intended for both physical and virtual goods purchases.

It relies on the SAS protocol for both types of transactions and the end-user handles the entire transaction cycle from the UPTD 102. This version of the UPTD 102 as a functional set could be embedded in a mobile phone device 102 that is equipped with a some local wireless communication link (e.g., WLAN or Bluetooth).

[0360] Other devices variants 102 which can be used as a UPTD 102 are now discussed.

[0361] One device 102 is a variation of the UPTD 102 without the display and the buttons. Such a device 102 can be made to be considerably smaller than a UPTD 102 because of the lesser power requirements due to the lack of a display (which would lower the battery size requirements) and the additional size of the display and the buttons. When the user is using this device 102 the user first authenticates herself to the device 102 using a biometric feature (e.g., using the fingerprint sensor) and upon successful user authentication, the device 102 executes the merchant authentication protocol. After the user of the device 102 has been authenticated and the device 102 has authenticated the validity of the merchant, the device 102 transmits its device 102 ID to the merchant. This transmission can be done using the two-way wireless capability of the device 102 or by activating a component that can transmit the device 102 ID (e.g., a RF ID tag, or a power-controlled barcode emitter). Instead of transmitting the device 102 ID, that biosensor activated component can transmit any other identifier that can be used to uniquely identify the user of the device 102, such as a (possibly encrypted) permutation of her social security number, or even some unique global identifier that the user herself does not know and need not remember. The transmitted device 102 ID (or other code) suffices for the merchant to query the transaction server for the records of the user of this device 102 ID, so that on a merchant device 104 mounted display (e.g. at the point of sale) the user can select which account to use for payment (as when the user uses the UPTD 102). The user authorizes payment using her PIN, as if using a UPTD 102. Since only aliases of the user's accounts are displayed and since the user's real identity need not be displayed on the (potentially) public display the user does not jeopardize her privacy in this mode. Moreover, since the user has authenticated herself to the device 102, the merchant is guaranteed that the registered and authorized owner/user of the device 102 (which is also the owner of the accounts displayed) is attempting to perform the transaction that is being displayed at the POS. Further, the increased level of security, thanks to the biosensor-based user authentication on the device 102, is achieved without the STS 108 or the merchant maintaining a global database of biometric identifiers which would be both implementationally expensive and challenging, but also potentially undesirable to consumers who would oppose such a centralized repository. In other words, no user data (e..g., fingerprint) is stored outside of the user's UPTD 102 and can be kept private. Since it is stored locally, it would be stored in a tamper-proof manner. Although such a device is described, it is possible that a UPTD 102 (which by its design incorporates all the elements and functions described here) could be operated in the manner described for this alternative device 102.

[0362] A second device 102 is like the previous device 102 but without the two way communication channel, which would result to even lesser size because of the smaller size and power consumption of the communication chip. In this case the user does not execute the merchant authentication protocol, thus this device 102 variation would be most adequate in situations where the user trusts the purported identity of the merchant. Except for the merchant authentication function the operation of the device 102 and the subsequent transactional functions are the same as described before.

[0363] A third device 102 is like the first described device 102 but with a less sophisticated biosensor. The biosensor need not compute the user verification locally (e.g., to match the known fingerprint of the registered user). In this case a secure communication is used to transfer the raw biosensor data (or some other representation of the raw data that is functionally equivalent to the raw data, for the purposes of the matching algorithm) to the merchant 104 and device 102 and eventually to the secure transaction server along with the device 102 ID or the user's globally unique identifier. The secure transaction server contains the stored bio-data (or their functional equivalent) for the individual associated with the device 102. The association code is used to limit the need for searching the entire database to produce a match. After the registered user of the device 102 (and device 102-associated account holder) has been matched successfully to the provider of the biosensor data, the operation and transaction of the device 102 proceeds as described for the first device 102.

[0364] The described devices 102 are progressively smaller in size and power requirements. As a result, except for the credit form factor, form factors such as a key ring are also possible and feasible.

[0365] As is the case with the UPTD 102, each of the described devices 102 and their function can be incorporated in a mobile phone. One particular example of a mobile phone used as a UPTD is a mobile phone that can display barcodes, or with a RF-ID attached to it, that does not include a local wireless link but delivers the functionality of a local wireless local link over the mobile carrier's network.

[0366] Finally, each of the described devices 102 can be thought of as modes of operation of the UPTD 102 that can be selected by the user, or automatically invoked with the aid of some automated or user-controlled identification of the scenario that each mode is best suited for.

[0367] Figures 51 to 56 show examples of a UPTD 102's display during pre-purchasing, physical goods purchase, and service purchase. When the display of the UPTD 102 displays "U P T D" on top of the display, this is meant to indicate that whatever is displayed is generated by the purchasing application running on the UPTD.

[0368] Fig. 51 shows example UPTD 102 displays for a pre-purchasing phase 600, including merchant discovery 602 and connecting 604 to a merchant 604, prior to interacting 606 with a merchant.

[0369] Fig. 52 shows example UPTD 102 displays for a physical goods purchase 610 (as in Fig. 8). The purchasing scenario is one of paying for a previously placed (and presumably consumed) order at a restaurant, in which the UPTD 102 initiates 612 purchase order acquisition, prepares and forwards a REQuest 614, and prepares and forwards an AUTHorization 616.

[0370] Fig. 53 shows example UPTD 102 displays for a physical goods purchase 620 (as in Fig. 8). The purchasing scenario is one of paying at the register of a convenience store, in which the UPTD 102 initiates 622 purchase order acquisition, prepares and forwards a REQuest and an AUTHorization 624.

[0371] Figure 54 shows example UPTD 102 displays for a physical goods purchase 630, in which the UPTD 102 initiates 632 purchase order acquisition, prepares and forwards a REQuest 634, and prepares and forwards an AUTHorization 636.

[0372] Figures 55 and 56 show example UPTD 102 displays for a service purchase 638, 650 (as in Fig. 9); token creation is not observable by the consumer. The purchasing scenario is one of buying tickets for a movie and using them to enter a movie theater.

[0373] Referring now to Figure 55, the UPTD 102 executes purchase order acquisition 640, then a REQuest 643, and an AUTHorization 644.

[0374] Referring now to Figure 56, which shows an example 650 of token verification and consumption in a service purchase, the UPTD 102 executes token consumption 652 and Service Granted 654.

Acquiring the device 102

[0375] The user would acquire the special purpose device 102 in much the same way that a user currently obtains a credit card: it was offered to him/her by a merchant, a financial institution such as a bank, VISA, AMEX, etc. It is also possible that the user might purchase the device 102; in such a case, the device 102 cost will be heavily subsidized, as is the case with mobile phones, by parties who stand to benefit from the ubiquitous availability of the device 102.

[0376] If a PDA or a mobile phone is used as a UPTD 102, the consumer will either download and install the purchasing application or this application might be pre-installed prior to acquisition of the PDA or mobile phone.

[0377] The user will typically carry the device 102 in her person.

[0378] After acquiring the device, the consumer has to enable the device for purchases. For that purpose, three relations must be defined. These are:

[0379] Register device 102 with the Secure Transaction Server

[0380] Identify authorized user of the device 102

[0381] Identify credit cards and bank accounts that can be charged from the device 102

[0382] Issue PIN to the user

[0383] For that purpose after downloading the software on the device (not necessary if the software is pre-installed) the owner of the device will have to register the device with the entity operating the STS. The software of the device will supply the user with the DID of the device. The user will (over the phone or through the web) supply the DID to the operator of the STS and register at least one financial account for making payments through the device, with the operator of the STS. Upon successful execution of these steps the device user will be issued a PIN (or receive the PIN by mail) to use for performing purchasing transaction with the device. At the beginning of this process the device is not associated with any financial accounts, so even if a party different that the owner of the device attempts to register the device and associated it with financial account they will only be able to do so in as much as they submit information about accounts that they own.

[0384] The process will be facilitated if the user has already established an online payment service account, such as a PAYPAL (paypal.com) account, C2IT (c2it.com, from Citibank), or another. Generally speaking, online payment services act as clearinghouses for moving payments between different accounts (bank accounts and credit cards). Usually the identifier of a real person is already in an electronic form, such as an e-mail address. A user of such a service sets up an account and associates credit cards and bank accounts with the e-mail address of the user. The user has to verify that she can access these accounts. Payments using a PAYPAL account can be charged against either a credit card or a bank account. Also, credit card or bank account payments can be received by the user and debits or credits can be withdrawn from or deposited to the user's chosen bank account. Additional credit cards and bank accounts can be added or deleted by the user through well established procedures of the online system.

[0385] The PIN need not be stored on the device 102 permanently. It suffices that the STS 106 knows it. The PIN will be used in order to authorize transactions from this device 102 (similar to a credit card PIN). In general, operating the device 102 requires authentication for two purposes: operating the device 102 (turning it on, viewing records, browsing service spots and services), and authorizing transactions. Each of these two types of authentication could be performed with either a PIN or some biometric method. Which method to be used for each authentication will be

decided by individual UPTD 102 manufacturers. For the purposes of this document, one assumption is that a biometric method is used to authenticate the operator of the device 102 and that a PIN is used to authorize transactions from the device 102.

[0386] If the device 102 was issued by a bank, his association will not be necessary because the bank will have established it prior to device 102 issuance. The combination of DID, PIN or biometric (operator and operation authentication feature) and user account identity all need to be valid for a transaction to be successfully completed.

[0387] Resetting the device 102 should erase the association with operation authentication feature and the associated account identity along with all the stored (if any) usage data. Thus if the device 102 is to be reset, it would have to be re-initialized. Similarly, if the device 102 is lost or stolen, it cannot be used without the biometric security feature; even if the biometric feature is successfully circumvented, no transaction authorization will be possible without the proper PIN. The only option is to reset the device 102, which would require its re-initialization. Of course this does not prevent theft of the device 102 but in order for the device 102 to be used again a new real-world identity would have to be associated with it. Since the UDID remains the same, the future user of the device 102 could be easily identified. Of course, since the STS 106 expects the UDID of the device 102 to be associated with the rightful owner of the device 102, a reset device 102 can not be used without proper action by the STS 106.

Using the device 102

[0388] After initialization, the device 102 is ready for use. It is expected that due to its form factor, the user keeps the credit card-sized device 102 in her wallet. As mentioned, one assumption is that of a single unique user per device 102. As the user approaches an "enabled" area, she might choose to turn the device 102 on. An "enabled area" is a specific location where a service is offered through wireless communication.

[0389] An "enabled area" is referred to as a "service spot". Examples of service spots include: movie theaters, parking lots, airport ticket counters, toll booths, mall stores, restaurants, etc. After turning the device 102 on, while within a service spot, a user sees a listing of available offered services. The user then selects a service to interact with. The typical service involves the purchase of goods and services, either of which is referred to as "virtual goods" (toll tokens, movie tickets, etc.), or physical goods, such as clothing, books, etc. The user's interaction with the service is expected to be similar to browsing. If at some point the user decides to make a purchase, for example to purchase a movie ticket, the user selects and confirms the transaction by selecting the purchase button and entering (to the device 102) her PIN (and/or biometric if available). Upon completion of the transaction, the user will receive a confirmation of the successful execution of the transaction on her device 102. Such confirmations may be stored locally on the device 102 for the user's convenience. No actual account numbers are stored on the device 102; only aliases for the accounts are stored on the device 102.

[0390] Access to such records will require user authentication by the device 102, as is the case for any usage of the device 102. As an additional security measure the device 102 will shut itself off after a set period of inactivity and user authentication will be required to re-activate it.

[0391] Typically the service spot has a live connection to the Internet and specifically to the Secure Transaction Server, or STS 106, in order to complete the transaction (user is notified accordingly if connectivity exists 106 or not). It is also possible for the merchant to choose to assume the risk of engaging in a transaction for which a confirmation is unavailable by maintaining an intermittent network connection (similar to what merchants often do with credit card processing). As an additional deterrent for use of the device 102 with insufficient funds, a typical online account includes credit cards that can be charged against transactions for which funds are not available in the user's primary online sub-account (typically a bank account). Finally, if the service spot has a live connection, the merchant may choose to offer an additional service, namely real-time access to a user's online account, so that the user can check balances and past transactions upon (or before) transaction confirmation (similar to checking the status of a PAYPAL account when connecting through a PC).

[0392] The user can disable the device from being used for purchasing following a process similar to registration. Upon supplying the DID, the issued PIN for the device and the account and password info for the Online Payment Service account associated with the device (or those of other financial accounts) they can choose to permanently or temporarily disable the device from being used for purchases using the associated financial accounts. Re-enabling the device will require a registration process.

Merchant experience

[0393] For the merchant that is offering a service spot, the following dimensions of setting up and maintaining a service spot are examined. The merchant has to set up a service spot, which includes the following actions:

[0394] Set up wireless access points (APs) that provide coverage for the area where the service is offered. One assumption is that a service is offered at the service spot where the physical merchant is. In other words, if a movie

theater is selling movie tickets, then the theater's service spot covers the area surrounding the movie theater. However, there is nothing preventing the proprietor (or an agent) of the movie theater to offer the service at another service spot, for example the enabled area of downtown Baltimore. There are many business reasons for doing this, for example cross-selling of goods and services (while in a parking garage in downtown Baltimore, reduced parking fee is offered if the driver purchases tickets to the nearby theater). Typically a merchant will pay a fee for such usage of another merchant's service spot (one analogy is to think of service spot hosting as web hosting, or similar to say YAHOO stores).

[0395] Provide internet connectivity for the service spot network (preferably continuous)

[0396] Become a UPTD 102-service merchant, which is a process similar to becoming a credit card approved merchant in order to accept and process credit card transactions.

[0397] Install and customize the service software on a Merchant Server (MS) that resides locally with the merchant. The MS can also be located on a remote server

[0398] Establish an association and communication with the Secure Transaction Server (STS 106) and register and initialize the merchant services with the STS 106

[0399] Publish the services that will be available through the service spot (a process similar to setting up a virtual store on the web)

[0400] Optionally offer charging stations, so that if the user device 102 power is low a customer can use the station to conduct a transaction.

[0401] The entire process is similar to the process of becoming a credit card merchant and deploying a Point of Sale (POS). For merchants that already have a POS the primary issue is the integration of the service spot infrastructure with the existing POS infrastructure.

[0402] One expectation is that larger merchants will typically seek the services of integrators in a way similar to deploying a POS today; after all, the service spot is an additional component in today's often complex POS systems. Smaller merchants have the option of deploying a service spot which serves as the entire POS by outsourcing all the POS processing to an application that resides behind the STS 106. For merchants with simple enough needs and requirements, a "do it yourself model" may be implemented where merchants publish services to their service spots by accessing a web service that can upload updates to their terminal, or by publishing them locally through a scaled-down laptop-like device 102 that connects to the MS.

[0403] Given the non-negligible overhead, it is expected that the first wave of merchant users would be national chains with multiple retail outlets. As illustrated later, there are significant advantages to adoption for such merchants.

Applications and Application Categories

[0404] Examples of applications that are enabled by the ubiquitous availability of the described devices 102 and services of the UPTF of the present invention are now discussed.

[0405] Broadly speaking, the device 102 can be used to make purchases of goods and services, either "virtual" ones, such as a ticket or paying for tolls, or physical ones, such as clothing, magazines, meals, etc. The user experience for each case is now discussed.

Purchasing "virtual" goods

[0406] Consider the case of purchasing a movie ticket. An assumption is that the service is offered at the service spot where the good can be "consumed", which can be extrapolated to the more general case (that is, the good being offered at a location different than the location where the good is consumed).

[0407] A user approaches a virtual counter (service spot) of the movie theater, activates the device 102, browses through the available shows, selects a show and show time to purchase a ticket for and purchases the ticket. Upon confirmation of the transaction the user can continue as if physically receiving the ticket. When the user enters the movie theater turnstile (where usually the usher is picking up the tickets), the ticket is "delivered" from the user transaction device 102 to the "usher-replacement" merchant transaction server AP.

[0408] There are a variety of schemes that can be used to simulate the process of "receiving" and then "giving back" a ticket: the user transmits a transaction code that is matched by the merchant transaction server, or location determination technology is used to confirm that the user moved beyond a control point.

[0409] The same method can be used for buying tickets or checking in at airports. Due to identity authentication issues it is easier to imagine the process for already reserved tickets (similar to electronic check-in).

[0410] Another application is paying for sit-down restaurant meals. The diner can request the check, which is delivered to his/her transaction device 102. After inspection of the details, the user can add a tip and authorize the payment. Varying status information can be put on the merchant server to make it difficult for deadbeats to escape. The benefits include no waiting in lines to pay or for the waitress to bring the bill, then wander around with one's credit card, then return the check and credit card receipt, then have the user sign the receipt, then again wait for the waitress to return

and tear off the receipt or leave the credit card information lying on the table until the waitress picks it up.

[0411] A variation of this application is that of paying for tolls. The user experience is essentially similar to using systems like EAZY-PASS today, with the additional advantage that it can be used nationwide, unlike today's systems that are not interoperable. The user is driving and while approaching a toll area he/she activates the device 102. The toll service appears on the device 102 and the user authorizes payment for the toll fee. The transaction is automatically completed when the driver drives through the toll and exits the toll area (from the other end). In such a case some form of customer location information identification is also necessary. This method enables toll services that are based on distance driven, using mere AP's as opposed to manned stations and controlled exits. Since it is unsafe and perhaps impractical for a driver to operate such a device 102 while driving, the driver might select to enable the device 102 to automatically accept and complete toll transactions. This is called a continuous (or process) transaction in that authorization persists through multiple, possibly dependent transactions and involves some additional security constraints to be determined.

Purchasing physical goods

[0412] A consumer can use the card to buy "physical goods", such as a book or clothing from a "brick and mortar" establishment. The consumer can go through the process of either a self-checkout or a checkout similar to a credit card checkout but without requiring the user to give the credit card for swiping and then sign. The user experience will be similar to what was previously described. A device 102 for reading bar codes or entering prices is still also required. The system needs to be able to manage multiple users' shopping carts and associate each one of them with the appropriate device 102. In the case of physical goods, the user device 102 needs to be physically associated with the checkout of the goods "belonging" to the operator of the device 102. This can be done with a separate barcode or RF ID on the UPTD 102, or in some cases using location determination technology.

[0413] The following is a variation of physical goods purchase where users can order items for pick-up that are then provided by employees, as in a carry-out restaurant. In any store where users queue for service, such as a coffee shop or fast food restaurant, a method for users to place their orders and payments without a cashiers assistance is enabled with the UPTD 102. A user enters the establishment and immediately uses the UPTD 102 to place the order through a menu service, for example a large cappuccino, providing the user's preferred name (symbolic ID). The order transaction is accepted by the coffee shop service and indicates acceptance to the user and possibly the estimated wait time. The user authorizes payment and the coffee is given to the user when ready. Combining the above with location determination, will ensure that the order is delivered to the right table. This eliminates the necessity of the user waiting in line just to place the order. It also saves labor for an employee to take the order and accept payment, plus allows customer orders to be taken concurrently. Similar advantages occur at fast food restaurants.

Payment of bills or fines

[0414] A variation of the "virtual goods" and "physical goods" purchasing modes applies to cases where a user's identity is required for the payment amount to be decided. Such is the case, for example, of paying a fine at an MVA location. In order for the user to be presented (on her device 102) with the correct amount for her fine(s), the overall system needs to identify the identity of the user operating a particular device 102, associate that identity with the system-stored identity and then present to that user's device 102 (and only to that device 102) the relevant charges. The identifier used (e.g., SSN, or driver's license number) might vary from service spot to service spot, but the general method would operate as follows: since a user's identity information is not stored on the device 102 but only a proxy for that identity (in the form of the e-mail account or username required to access the online payment service), the device 102 would transmit that proxy identity to the service spot which in turn would query STS 106 (perhaps for a fee) for the necessary identifier (e.g., driver's license). One assumption is that this kind of information would be stored at the STS 106, as an element of the consumer's profile.

Other example applications

[0415] Applications include all the services of purchasing goods as described in the previous two sections. Some specific cases and variations of particular interest are discussed.

[0416] The UPTF framework makes it possible to offer merchant-sponsored real-time auctions for purchasing of goods and services.

[0417] Another application is that of offering hosted POS (point-of-sale) for merchants. Such a service could be deployed in order to jumpstart the usage of devices 102 by outsourcing the processing of such transactions for the merchants, in parallel with other paying mechanisms. A merchant could have only the wireless AP terminal/register, an Internet connection and no other in-store infrastructure and be able to accept payments from UPTD 102s. The

software package could include accounting, inventory, and other business applications.

[0418] Stores can offer the user transaction device 102 to customers, for them to use during their shopping experience. Such devices 102 could be used by anyone, but would need to be initialized (PIN and/or biometric and online payment account). Of course, it will be more suited for customers that already have an online payment account or even a device 102 that they happen to have left some place else. This would introduce the device 102 to new consumers ("take it home for a drive").

[0419] The device 102 can also be used as an intermediary for different online payment systems. Similarly, an alternative business model would be to bypass the online payment system, so that the UPTF becomes its "own" online payment system and clearinghouse for executing the transactions within the banking system network.

[0420] Another application is that of UPS or FEDEX drop-off boxes that can accept payments from the device 102, as opposed to the current mechanism of either maintaining an account or using a credit card and filling up the necessary information on the packing slip. The drop-off box could include a screen for user entry of the destination zip code so that the exact charge can be decided (otherwise the user consents to the appropriate charge to be charged to her account whenever this charge is assessed, which is the currently used scheme). Also the zip codes and priorities of deposited packages can be conveyed in real-time to the carrier's system in order to optimize pick-up routes or to incorporate the information in the planning system.

[0421] Also, another variation of the carry-out service would be to use the device 102 as a "take a ticket" service for service where customers keep track of their place in a line (queue) using "first come, first serve" tickets. This could be coupled with a notification service that informs users of estimated waiting time and a notice when their time for service is up. Such a system could be used in theme parks to avoid waiting in lines and even coupled with a location-aware service that estimates travel time to the location that the service is offered.

[0422] Additional services can be offered on-the-fly in existing service spots, for example, a fund-raising effort in a crowded space, such as seeking donations to charity in a public area or a crowded movie theater prior to beginning of the feature film.

[0423] The device 102 can be used as a secure e-commerce terminal by simply connecting it to a computer (USB, PCMCIA, etc.) or simply to a gateway which will also provide the network connectivity. The device 102 can then either be used as in the wireless case, or as an identification card. In either case, it provides a viable solution to the huge problem of credit card fraud on the internet which primarily victimizes the merchants (who have to absorb the cost of fraud). In that case the business model is transaction based, as the merchant receives the benefit of a much reduced risk of a fraudulent transaction. Merchants who do business on the internet are currently charged significantly more per transaction due to the much higher fraud risk.

User benefits

[0424] Benefits for end users are now discussed. A purpose and benefit of carrying and using the device 102 is that it facilitates conducting financial transactions. This benefit is more evident when purchasing goods or services where no exchange of physical goods is necessary (such as a toll token, or ticket). Combining location-specific identification of the device 102, the user can achieve a faster transaction cycle and automated checkout. It is easy to select between accounts and balances/status are instantly available at any time. Additionally, the device 102 is non-intrusive for the user, since the user can choose when to use it. The system permits a true paperless transaction. Another benefit of the device 102 is that it can be used for small transactions where typically a credit card transaction would be infeasible. Overall the user could use the card as a replacement for the need to carry cash or any other card and eventually the wallet.

Merchant benefits

[0425] A benefit for the merchant is that the entire transaction cycle is much faster and thus a cheaper alternative to current means, because fewer people are needed to satisfy the transaction processing needs of the merchant. An added benefit for the merchant is that this way they can reach more users especially during busy times through concurrent automated processing of sales transactions. It is no longer a one-to-one relationship between cashier and customer. The load of a typical store is pretty irregular, with higher volumes occurring on weekends and at the end of the workday. Crowded checkouts deter potential buyers especially since more affluent buyers (higher spend per person) are more sensitive to time and are discouraged by longer waiting lines. The system permits a true paperless transaction. In some case the merchant will be able to maintain a cashier-less store, or to incorporate self-checkout capabilities thus further reducing the load during busy times. Certain other merchants will also benefit from the ability to conduct quick small cash transactions.

[0426] Another class of beneficiaries includes financial institutions (for example, credit cards like MasterCard and VISA. For them, an advantage of such a device 102 is that it is more secure than current credit cards. Credit card fraud

plus the cost of lost credit cards (the consumer typically does not pay for transactions occurring after the loss of a credit card) is a huge amount for these institutions and in fact they have been experimenting with smart cards as a replacement for existing credit cards. The UPTD 102 significantly improves the secure use of credit cards and will result in lower credit fraud costs.

[0427] Fraud accounts for 0.08 to .09 % of all credit card transactions in the offline world (fraud accounts for 0.25% of credit card transactions over the internet. Given the total value of credit card transactions (close to$3T), fraudulent transactions amount to$2.4B annually.

[0428] The UPTD 102 can reduce fraudulent use of a card when in proximity to the store or if it is used when attached to a computer accessing the network, for typical e-commerce transactions.

[0429] The UPTD 102 device 102 and associated methods and infrastructure of the present invention provide a device 102 that can be used by, and carried by, everyone, does not require familiarity with computers and their workings and process-wise it is a portable identity medium that can be used to authorize and execute transactions. In fact, financial, or financial task-related transactions are the only "universe" that the user is exposed to. Ease-of-use, ubiquitous presence and speed are the main features of the type of e-commerce provided by the UPTF of the present invention - that is, pervasive commerce.

[0430] Features of the present invention include:

[0431] The device 102 introduces convenience for both consumers and participating merchants. Consumers need only carry a single device 102 and be able to use any account for a purchase, all while they can check-out faster, often without the need of interacting with a person, or, in some cases, check-out without cashier assistance. Merchant benefits include achieving faster transaction cycles, reducing the cost of running check-out stations and lowering the risk of credit fraud, whose cost they are eventually accountable for.

[0432] The discussed business models associated with the commercialization of the device 102 focus on collecting fees per transaction, while acting as an intermediary to the transaction cycle. The justification of the fee is the tangible benefit for the participants to the transaction: convenience and efficiency for consumers and savings and efficiency for merchants. Another class of revenue streams is associated with hosted value-add services, such as real-time offers and incentives to customers that are about to make payments and cashier-less stores for merchants.

Summary

[0433] In summary, the present invention enables consumer to purchase (order and pay), wirelessly, and from a distance, at physical Points of Sale (physical stores), for goods and services, using any of their financial accounts and it enables them to do so securely, quickly, using a PDA, a mobile phone or a custom device with limited hardware, all while the device stores no user and account information. Security relies only on a 4 digit PIN that is not stored on the device. The device can be disabled from purchasing very easily by the user himself. The process of enabling a device for such purchasing and further managing the device for such purchases poses minimal management requirements to the user.

The Secure Pervasive Transaction Protocol

[0434] The Secure Pervasive Transaction Protocol is disclosed in SECURITY FRAMEWORK AND PROTOCOL FOR UNIVERSAL PERVASIVE TRANSACTIONS, U.S. Serial No. 10/458,205, Attorney docket number 1634.1003, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed June 11, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference. A description of the Secure Pervasive Transaction Protocol (STP) is now presented, after a brief description of other security algorithms.

[0435] Symmetric cryptographic schemes (or algorithms), in which encryption and decryption use the same key, are well known in the art and have several desirable characteristics such as ease of key management and lower computational requirements as compared to asymmetric cryptographic schemes.

[0436] Many current security mechanisms employ asymmetric cryptographic schemes, such as the public key systems with their associated Public Key Infrastructure (PKI) systems and are known in the art. However, the PKI (Public Key Infrastructure) system of the related art includes specific costs associated with creating and maintaining this infrastructure. Examples of these costs include key distribution, management and storage.

[0437] The asymmetric encryption/decryption algorithms used by the PKI systems involve relatively complex and time-consuming computations. Hence they are not well suited for economical and compact mobile computing devices on which only limited computing resources and battery power are available.

[0438] Symmetric algorithms consume substantially less computing power than asymmetric encryptions and decryptions. Communicating parties in symmetric cryptographic systems typically share the same key, which is then used by them as a parameter to encrypt and decrypt the message data.

[0439] The part of the Securee (or Security) Agreement Submission (SAS) protocol (also referred to as the Secure

Pervasive Transaction Protocol (STP)) relating to the present invention discussed herein above is now discussed with reference to Figures 57-63.

[0440] The SAS protocol relates to a method of a third party (verification party) verifying an agreement between two distrusting parties (agreement parties) in an insecure communication environment. The SAS protocol extends to a multi-party agreement method, where a verification party verifying an agreement among multiple (more than two) distrusting agreement parties in an insecure communication environment.

[0441] The SAS protocol is a computationally lightweight protocol carrying agreement data and other sensitive messages between distrusting agreement parties and a verification party in an insecure communication environment so that the agreement data is protected during the transmission and the agreement data can be shown to be consistent. The protocol of the present invention satisfies security properties such as privacy, authentication, user anonymity, non-replayability and non-repudiation.

[0442] The Secure Agreement Submission (SAS) protocol that is designed for use in unreliable communication environments, such as wireless networks. The SAS enables multiple parties to an agreement to submit the agreement information to an independent verification party in a secure fashion over these unreliable communication channels. In addition, the SAS provides a mechanism and procedures comparing and verifying the agreement information and notifying the participants of the results, also in a secure fashion. As is disclosed herein below, the SAS protocol is ideally suited for many types of transactions such as purchasing goods, wireless voting, virtual token collection and many others.

[0443] The SAS includes a cryptographic scheme based on a family of symmetric cryptography algorithms, in which encryption and decryption use the same shared key. The SAS includes a novel key derivation and generation scheme that can be used with many symmetric cryptographic schemes and results in several new, desirable properties for the protocol, such as a high degree of security in a non-secure communication environment (such as a wireless channel), low computational complexity and no need for a user to store or transmit keys, or other personal identification data pertaining to the attempted agreement, such as username, account data, etc.

[0444] The key generation scheme of the SAS uses a mobile computing device capable of communication. The mobile computing device executes the protocol and accepts input from a user. Such devices can be special purpose devices or readily available computing platforms such as Personal Digital Assistants or programmable cellular or mobile telephones.

[0445] The key derivation algorithm combines information about the mobile computing device with information about the user of the device. The algorithm also combines information that is stored digitally by the device and the shared secret information that is input by the user. Such a combination ensures with high likelihood that only the intended parties are able to decrypt and thus access the communicated data. If a device is lost or stolen, it can not be used without the specific user input information, which itself is not stored on the device. The deterministic key derivation algorithm may be generally known. The set of stored parameters is preferably known only to the device and the verification party, but if generally known are not sufficient to determine the key, without knowledge of the shared secret value. The secret value, or the stored parameters, or the key are never transmitted in a message. What is transmitted is a message parts of which are encrypted with a key that is derived from the stored parameters and the shared secret information that is input by the user.

[0446] An agreement, with respect to an application, is a general statement between parties for which a verification procedure can be executed to provide confirmation that the parties have a common understanding of the statement, within the context of that application. For example, a financial transaction agreement could be that "Party A will pay Party B$X for Item Y." An agreement statement is represented by agreement data, the contents of which are not defined by the invention but by the needs of the application.

[0447] The protocol is referred to as the Security Agreement Submission (SAS) protocol, to accomplish the agreement verification. An aspect is an SAS encryption (SASE) mechanism that provides many security properties in an insecure communication environment. The SASE is used to encrypt and decrypt all messages that are part of the SAS. The SASE mechanism is implemented by each of the agreement parties and the verification party.

[0448] The SAS achieves the following desirable security properties:

[0449] Authentication of agreement parties: The identities of the involved agreement parties can be determined to be who they claim they are, to a high degree of likelihood by the verification party, based on the fact that a SASE coded message sent by an agreement party can be decrypted and understood by the verification party, using a decryption method with a key that is specific to the sender and only known to the verification party and the specific agreement party.

[0450] Authentication of verification party: The identity of the verification party can be determined to be who it claims it is, to a high degree of likelihood by each individual agreement party, based on the fact that a SASE coded message sent by the verification party for a particular agreement party can be decrypted and understood only by that agreement party using a decryption method with a key specific to the agreement party and only known to the agreement party and the verification party;

[0451] Anonymity: The agreement parties may remain anonymous to each other, if desired in an application through

the use of the SASE method.

[0452] Privacy of Agreement: The agreement data sent between the agreement parties and the verification party is protected by SASE so that, if intercepted, no party other than the intended receiver is able to decrypt and read the data. Similarly, response messages from the verification party to the agreement parties are protected.

[0453] Tamper-resistance: The agreement data sent between the agreement parties and the verification party is protected through the use of an encryption signature so that no party can alter the data sent by other parties without a high degree of detection.

[0454] Non-replayable: Agreement data sent between the agreement parties and the verification party (if intercepted) is protected by an encryption mechanism that incorporates the value of the time when the agreement transaction occurs, and such a timestamp is also included in each message and recorded by the verification party. Thus, no party can replay the agreement data to forge a new agreement because each key is associated with a specific timestamp which is recorded by the verification party in a message log.

[0455] Non-repudiation: An agreement party can not later claim that they did not generate an agreement message that has been verified by the verification party except under certain specific conditions that are highly unlikely. These security breeches include the case, where all the secret parameters (the device-specific stored parameters and the shared secret which is input by the user of the device) have been divulged or discovered and the mobile-computing device has been used without the consent of that agreement party. It is also possible for the verification party to generate a false agreement, but it would involve the collusion of the verification party and the other parties to the agreement, which is also highly unlikely. In addition, the verification party will keep records that record the sequence of SAS message exchanges involved in each transaction.

[0456] Agreement Group Authentication: The SAS ensures the integrity of the agreement party group (the group consisting of and only of the parties among which the agreement is conducted) so that no other party can pretend to be an agreement party or an agreement party can pretend not to be an agreement party. This is accomplished explicitly by a membership list and identity cross-referencing. It is also assumed that all participants in the agreement are a priori known to the verification party and able to be individually authenticated.

[0457] Agreement Verification: The agreement is verified to be consistent among the authenticated agreement parties through the use of redundant and cross-referencing information contained in the agreement data and the use of a verification procedure consisting of basic matching rules and specific matching rules that may depend on the application.

[0458] Computational Efficiency: The security mechanism of the SAS is based on private key (symmetric) cryptography that is more efficient than alternative methods.

[0459] Physical Security: The security mechanism can be implemented so that it is not necessary to store all of the necessary encryption information on the client mobile computing devices, thus making it easier to protect the secret information if the device is compromised. Specifically, the shared secret input by the user is not stored on the device. Also, when the device is used in a particular application context, user-identifying information is not stored on the device. For example, when the device is used for purchasing goods and service in physical retail stores, the name of the consumer, or the user's account information is not stored on the device.

[0460] Intrusion Detection: The security mechanism is centralized through the use of an independent verification party so that attempts to use the system by unauthorized users that rely on multiple access attempts are easily detected and handled accordingly.

[0461] With the above-mentioned aspects, the SAS is ideal for being used as a vessel to carry financial transaction data between distrusting parties in an insecure communication environment. It is also well-suited for a system using low-cost user devices, which have limited computing resources.

[0462] The SAS is now explained with reference to Figures 57-63.

Architecture

[0463] The overall architecture of a system 1100 for agreement verification between two parties using the SAS is shown in Figure 57. The system 1100 comprises two Agreement Parties, AP1 (1101) and AP2 (1102), an Agreement Communication Channel (1103), the Authentication and Verification Party AVP (1106), a Transaction Communication Channel (1113) and Transaction Processing Component (1116). The AVP 1106 itself comprises four components, the View Gathering Module (1108), the Agreement Authentication Module (1118), the Agreement Verification Module (1112), and the User and Device Database (1114).

[0464] Referring now to Figure 57, AP1 1101 generates agreement information in the form of AP View 1 (1110) and AP2 1102 generates agreement information in the form of AP View 2 (1120). The Transaction Processing Component 1116 and its associated communication channel are included to further illustrate the application environment for the SAS. It is assumed that the Transaction Communication Channel 1113 is a reliable and secure channel.

[0465] The SAS assumes that the Agreement Channel 1103 is a reliable, although insecure, communication channel

between the APs 1101, 1102 and the AVP 1106. All messages that are part of the SAS protocol are encrypted/decrypted using the SASE. In addition, the AVP 1106 is considered to be located in a secure facility, so that the sensitive information in the User and Device Database 1114 is sufficiently protected.

[0466] The SAS agreement verification process is described as the following six functions. More details of each function are provided in the later sections:

[0467] Function 1: Each Agreement Party (AP) 1101 or 1102 creates the AP View 1110 or 1120 including agreement data and additional parameters. Sensitive portions of the view 1110 or 1120 are encrypted using the SASE. The AP View 1110 or 1120 is digitally signed by the AP 1101 or 1102, respectively. An Agreement Message is created from the view 1110 or 1120 and then transmitted to the Authentication and Verification Party (AVP) 1106 using the Agreement Communication Channel 1103.

[0468] Function 2: The AVP 1106 receives the agreement messages from the APs 1101 or 1102 and delivers them to the View (or Agreement) Gathering Module 1108. The View Gathering Module 1108 determines that this is a two-party agreement and when it has received two agreement messages (one from each party) for this particular agreement. The messages are then passed to the Authentication Module 1118.

[0469] Function 3: The Authentication Module 1118 authenticates the agreement parties by using the SASE to decrypt the agreement messages, and determines that the signed agreement copies are indeed signed by the involved APs 1101 or 1102. This is done through the properties of the SASE scheme and using the information stored in the User and Device Database 114. If authenticated, then the decrypted messages are passed to the Agreement Verification Module 1112. If the authentication fails, then the results are sent to the Agreement Parties 1101 or 1102 as indicated in Function 6.

[0470] Function 4: The Agreement Verification Module 1112 executes a set of matching rules that check to determine whether the agreement data in each of the agreement messages 1110 and 1120 is consistent with each other. There are several matching rules that are always applied as well as an interface for application-specific rules. Together these matching rules are checked to verify that the agreement data included in all received copies of the agreement is consistent. Typically, in each agreement message there is reference to the other parties of the agreement and possibley a reference to a user identity that is not public information (for multiple users per device case). In addition, each application can provide a plug-in function to verify that the application specific contents of the agreement received from the agreement parties agree with each other. For example, in a financial transaction, there is an agreed upon amount that can be matched among the parties. If there is no associated transaction processing, then the system proceeds to Function 6. Otherwise, Function 5 is then executed.

[0471] Function 5: In many applications, once the agreement details have been verified, it is desirable to perform some services based on the contents of the agreement. In this case, the decrypted agreement data is passed to the Transaction Processing Component 1116 to execute these services using the Transaction Communications Channel 1113. The Transaction Processing Component 1116 will typically create response messages for each agreement party following the processing of the transaction. The response messages are communicated back to the Agreement Verification Module 1112 through the same channel.

[0472] Function 6: The Agreement Verification Module 1112 creates a Response Message for the Agreement Parties 1101 or 1102 that includes the results of the verification. If there is a response from a Transaction Processing Component 1116, then this is also incorporated into Response Messages. The Agreement Verification Module 1112 passes the response messages to the Agreement Authorization Module 1118 that uses the SASE to encrypt response messages for the Agreement Parties 1101 or 1102 and transmit the response messages to the agreement party 1101 or 1102 over the Agreement Communication Channel 1103.

[0473] The agreement method is summarized herein above. However, in order to operate such a system 1100 implementing the agreement method , there are several additional functions that occur. Prior to joining an agreement, any AP 1101, 1102 who wishes to use the verification service must be registered with the Authentication and Verification Party (AVP) 1106. The registration process results in a user account being created for the AP 1101 or 1102 at the AVP 1106 and necessary information stored in the User and Device Database 1114. A registered AP is hence known as an AP User of the system.

[0474] Registered APs 1101, 1102 are assumed to employ devices, called AP Devices or Client Devices. Each device is capable of carrying out the computations necessary for the verification procedure (including the encryption of outgoing messages and decryption of incoming messages intended for this particular device) and of reliably communicating with the AVP 1106 over the Agreement Communication Channel 1103. Each device is also registered at the AVP 1106, together with the key derivation parameters stored in the device (e.g., pseudorandom number generator and its seed, etc). In addition, the association between the AP users and their devices is also stored in the User and Device Database 1114 at theAVP 1106.

[0475] It is possible to allow the cases where each device may have multiple AP users associated with the device or each AP may be associated with multiple devices. Depending on the requirements the application , the multiple users per device may or may not be permitted. For instance, if a particular application issues one and only one device

for each registered AP user, it is no longer be necessary for the AVP 1106 to distinguish the user from the device and the data items for each user may be stored together with the data items for the device issued to the user. During normal operations, the system 1100 may use the identifier of either as a reference to locate these data items. This results in more efficient processing than in the multiple user case.

[0476] The User and Device Database 1114 is also used to log and store the records of each agreement session by recording the SAS messages to and from the agreement parties 1101, 1102 and the AVP 1106. Each such agreement transcript can be accessed by the user, device or transaction IDs. This can be used to prevent replay of transactions by reusing a timestamp and to resolve potential claims regarding the verification procedure and the parties involved.

Security Protocol

[0477] The security protocol, termed the Secure Agreement Submission Protocol (SAS), is explained in more detail in this section. As part of the description the terms used in the protocol are defined.

[0478] Device ID (DID): A unique identifier for each AP (client) Device involved in the agreement generation, transmission, authentication, and verification. This ID is public in the sense that it may be included in messages as plain text, i.e., in non-encrypted form and that it is placed in the non-encrypted part of the message. It can also be used as the address of the device during communication. For instance, the physical address of the network interface (MAC address) of the device can be used for this purpose.

[0479] **User ID (UID):** A unique identifier for each registered AP entity involved in the agreement. That is, the human or entity using an issued AP client device involved in the agreement generation, transmission, authentication, and verification. This UID is used to identify the current user of an AP client device and there is a one-to-one mapping between the UID and an account opened at the AVP 1106. This piece of information is private in the sense that the UID must not be transmitted in plaintext during the protocol execution. Examples of a UID include a name, an e-mail address, a driver's license number, or some account id. The UID is only needed in case the client device has multiple users and is needed to identify the specific user (of many) of the device that is attempting the transaction. The UID may or may not be stored on the device depending on the security needs. If the device has only one registered user, the UID is unnecessary, thus allowing to not store any user-identifying information of the device at all.

[0480] **Private Identification Entry (PIE):** The shared secret input by the user. It is entered by the user whenever the user attempts a transaction. Preferably it is issued to the user following the registration of the user for the application that the client device is used for. It can also be selected by the user at such time. The PIE is an alphanumeric string. In order to speed up the user entry to make it easier for the user to remember it, the PIE can be a number such as 4-digit or 5-digit PIN. It is a piece of highly secure information in the sense that it is never transmitted during the protocol execution, it is only known to the user and the AVP 1106, and its secrecy should be well protected. It is assumed that the PIE can be input by the user on an AP device in a secure fashion or it may be deterministically generated using a biometric device such as a fingerprint sensor. For example, a computation applied on the fingerprint data received from the fingerprint sensor can be used to generate a PIE that is initially communicated to the AVP by the user. Whenever the user attempts a transaction, the user applies her finger to the fingerprint sensor, thus generating the PIE. The PIE is not kept in permanent storage on the AP device, but is used as an intermediate parameter required for the generation of the encryption key for a transaction and it should not be retained by the device for a period longer than the transaction execution time. If a particular implementation uses a form of PIE that is not convenient for a user to input for each agreement transaction and the device needs to store its user's PIN, the storage must be secure and tamper-resistant. The user's PIE is also stored in the User and Device Database at the AVP, which is considered to be a secure facility.

[0481] **Device User ID (DUID):** An identifier for each device to locally identify its users, if the application assigns multiple users to a single AP device. The mapping between the DUIDs of a particular device and the assigned users' UIDs is stored in the record of that device the User and Device Database at the AVP, as well as at the device itself. At the same time as a user inputs her PIE at an AP device, she shall also supply her DUID. The DUID is public in the sense that it may be transmitted as plaintext in messages. The DUID of the current user may be stored at the AP device during the execution of a transaction.

[0482] **Digital Signature (DS):** A digital signature associated with a message can be used to verify that a document has not been tampered with and that it was generated by the signer. For a given block of data, a message digest (MD) can be computed using a digest algorithm such as a Hash function. The resulting digest is then encrypted using the encryption key of the signer and the resulting encrypted block of bits is the signature. In order to verify a signature, the recipient decrypts the signature using the key of the sender. If the receiver generates a digest value from the received message which matches with the digest decrypted from the received signature, then the signature is accepted as valid and the received message is considered to be the original unaltered message.

[0483] **Random Sequence Number (RSN):** The RSN is a pseudorandom number that is generated from a locally stored pseudorandom sequence number function R (a pseudorandom number generator). Such RSN functions are well known in the art. Typically the generation of a pseudorandom number also involves another parameter, a seed S.

The seed is used as the initial input parameter for the generator R to generate its first pseudorandom number output. From then on, the generator uses the output from the previous iteration as the input for generating the new pseudorandom number. In the SAS , the RSN number may be generated either by an AP device or the AVP. Each AP device has its own R and S, which are securely stored on the device and at the AVP. On the AVP, given the DID of an AP device by which a RSN is generated, a program can deterministically locate the same pseudorandom number generator function R and the corresponding pseudorandom number generation seed S for that device from the User and Device Database containing information about all issued devices.

[0484] Timestamp (TS): The time associated with a transaction. It can be generated from a reading from a per-device local clock or delivered to the device on a per transaction basis. For example, if the device is used in a purchasing application, the TS can be the TS of the purchase order that the merchant and the consumer will agree on. The TS should be an element of an increasing sequence of values with a known and generally long period between repetitions of values. It is used for two purposes: as an indicator of a device's local time and as a parameter to control the pseudorandom sequence number generator of the same device. In the former case, the TS is used to prevent message replay, as no two messages from a given source should have the same TS. In the later case, the TS is used to control the number of iterations of the generator R before the final output is used as the next pseudorandom number by the SASE.

[0485] Transaction: The complete execution of one agreement transmission, authentication, and verification. On an AP Device, a transaction begins when the device generates its view of the agreement and ends when a receipt from the AVP is received and understood. A specific application might include multiple such transactions in order to accomplish the goal of the application. For example, if the application is that of a consumer purchasing goods or services from a merchant, a first transaction might be that of acknowledging and pre-authorizing the purchase and a second transaction might be that of confirming and authorizing the purchase after the completion of the first transaction (when an adequate response is received from the AVP)

[0486] Transaction ID (TID): A unique identification number assigned to an agreement. The method of generating the TID is generally application specific and it can be generated by one of the agreement parties or a component of the AVP, such as the View Gathering Module. The Gathering Module will use the TID and an additional parameter, Number in Transaction (NIT), that specifies the number of parties in the agreement, to identify when it has received a complete set of views for an agreement. In a two-party agreement, the TID and NIT may not be required.

[0487] View: The processed agreement data by an AP device. A view of an agreement consists of an encrypted portion and an unencrypted portion. The encrypted portion includes reference information (the other party's Device ID, and optionally the User ID, a message digest MD, which can also be digitally signed) and the specific agreement data. The unencrypted or plaintext portion consists of reference information including Transaction ID, Number in Transaction, Time Stamp, Device ID and Device User ID.

[0488] Agreement Data: The agreement data conveys the specific details that are agreed upon by the involved parties. For example, the amount that one party agrees to pay a second party is a agreement data. Agreement data may also contain information that is relevant to the agreement, but needs to be shielded from the other agreement parties. For example, the financial account with which one party agrees to pay the second party may be included in the agreement data, but this is not protected from the second party through encryption. The agreement verification module will be configured to determine that both parties agree on the amount and the participants, while protecting and delivering the other agreement data, such as the account information for the appropriate additional processing, such as by a Transaction Processing Component 116. The primary purpose of the SAS and the cryptographic algorithm is to protect the agreement data during transmission and to shield the other information from the other agreement parties, while providing the security properties of privacy, authentication, user anonymity, non-replayability and non-repudiation

[0489] The method 1200 of encrypting an SAS view , referred to as the SASE, is illustrated in Figure 58. The SAS view 1210 illustrated in Figure 58 corresponds to an AP View 110, 1120 of Figure 57. As shown in Figure 58, an AP view 1210 includes a cipher text part (or encrypted part) 1212 and a plaintext part 1214. The plaintext part 1214 includes the TID, the NIT, the DID of the AP device generating the view, the local TS of that AP device, the DUID of the current user of the device, the TID and the number of parties in the agreement. The encrypted part 1212 includes four fields: the digital signature DS 1216, the agreement, the UID of the AP, and the DID of the other AP involved in the agreement. The DID of the otherAP involved in the agreement is the minimum necessary reference field in order to provide the desired properties of the SAS protocol. The DS further increases the strength of the security by ensuring that no other party has tampered with or modified the contents of the view in any way. The TID and NIT are not necessary in a two-party agreement. The purpose of the TID and NIT is to associate views (messages) and responses to these messages and, alternatively, information that relates messages and responses to these messages can be provided as part of the agreement data itself in a way that depends on the particular application.

[0490] In the case that the AVP only allows one user to be associated with each device, the UID field may be omitted because the AVP can derive such a UID based on the DID. The UID of the other party involved in the agreement is

not included in any view, so that the other AP involved in the agreement may remain anonymous. The DUID field is also not necessary in this case.

[0491] At first, the DID 1234 of the view generating device and the TS 1236 obtained from the device's local clock or provided as a part of the agreement data, are input to the device's pseudorandom number generator 1252 to generate a RSN 1246. In the SASE, the TS 1236 is used to control the number of iterations of the pseudorandom number generator 1252. Only the final result after these iterations is used as the output RSN 1246 for the SASE.

[0492] There are several variations in how the TS is employed to generate the RSN. One method of using the TS to control the number of inductions is to use the difference between the TS value (in number of minutes or seconds) and another mutually agreed base time value as the number of inductions. The generation of RSN is denoted as: RSN = R (S, TS, T_o) where To is the base time. The base value T_0 is stored both at the AP and the AVP which will store the base value in the User and Device Database in the record for the AP device and is specific to each AP device. The mutually agreed base time is advanced on both the AP device and the AVP in order to reduce the number of inductions to produce a SASE RSN, as long as the advancement of the base time on AP and AVP can be synchronized. If desired, as the base time advances, the seed may also be updated. For example, the new seed S' may be the S' = R (S, T_0', T_0) where S is the original seed, To is the original base time, and To' is the new base time. The property of the SASE that needs to be maintained is that given a particular sender's pseudorandom sequence number generator R, its seed S, and the same TS value as used by the sender, the receiver can deterministically reproduce the same RSN as was generated by the sender

[0493] A hash function H 1254 is then applied to the output of two-argument function F that when applied to the locally generated RSN 1246 and the PIE 1248 input by the AP user outputs a single argument (typically a string), in order to create the encryption key K 1250:

$$K = H(F((PIE, RSN)) \text{ or further expanded to: } K = H(F(PIE, R(S, TS, T_0))).$$

Such Hash functions are difficult to invert and are well known in the art. The function can by any known function, such as a function that appends the PIE string to the RSN string, or XOR's the PIE and the RSN, etc.

[0494] A message digest function 1258 is applied to the data, the UID of the AP user, and the DID of the other AP involved in the agreement to generate a message digest (MD) 1216 of the view. The message digest function 1258 can be a hash function that takes as input the plaintext of these three data items and produces a single number. Such hash functions for use in producing message digests are also well known in the prior art. For example, the hash function SH1 is often used for this purpose.

[0495] The encryption algorithm with the encryption key K 1250 is then applied to the message digest 1216, the agreement data 1244, the UID of theAP user 1240, and the DID of the other AP involved in the agreement 1242 to generate the cipher text part 1212 of the view. The DID 1234 and TS 1236 which were used to generate the encryption key are also included in the view as plaintext. The TID 1230 and NIT 1232 are also included in the plaintext part 1214 of the view. Thus, the agreement view 1110 from the first AP device is the following:

$$\text{AP View 1} = \{TID, NIT, DID_1, TS_1, DUID_1, \text{Encryption}[K_1: \underline{(UID_1, DID_2}, \text{data}, \underline{MD_1})]\}$$

[0496] The specific encryption algorithm employed by the system 1100 can be any of the known symmetric key-based encryption algorithms chosen to provide sufficient protection. However, the SAS includes the key generation process to be used with the chosen encryption algorithm.

[0497] As one embodiment of the SASE, the encryption algorithm 1256 is TripleDES, the Random Number Generator 1252 is a Mersenne Twister, the seed is a 32-bit number, the timestamp is a 64-bit number representing seconds, the PIE is four digits, and the Hash function 1254 is SHA1 and the function F that generates the input to the Hash function, is a function that appends the PIN to the RSN.

[0498] For further protection, the SAS protocol uses message padding in order to further prevent "known-text" attacks. In "known-text" attacks, an attacker who knows the plaintext of the agreement will attempt to reverse engineer the encryption key and eventually, with enough successful attacks, the other parameters used by the key derivation process. If successful, the attacker becomes capable of reproducing the encryption key for that particular view. Since the key changes over time (each timestamp is associated with a new key), this attack would reproduce the key for that particular timestamp only. Further transactions using the same timestamp are denied through comparison with the previous transaction timestamps stored at the AVP.

[0499] The padding scheme will insert random bits before and after the real fields so that an observer cannot determine where the real data begins, increasing the difficulty of "known text" attacks. The amount of padding is determined by the lengths of the overall message and the included data. In one embodiment of padding 1300, as illustrated in

Figure 59, a padded field 1302 starts with a field of fixed length 1312, which describes the number of random bits inserted before the actual encrypted fields. This field 1312 is followed by a string of random bits 1314 of the length specified by this field 1312, and then the real data field 1310. Random tailing bits 1316 are also appended after the end of all encrypted fields to further increase the difficulty for an attacker to extract the real cipher text part of a view. Since the total length of each field is known, it is not necessary to specify the length and offset of the tailing random bits 1316. If the length of each field is not known, field 1312 will be followed by an additional field that specifies the offset of the tailing random bits 1316. In another embodiment, random bits are inserted only before and after all fields. In this case although the difficulty for an attacker to determine the location of each data field is reduced the processing of each SASE message is also reduced. Padding is applied before encryption is applied during view construction.

[0500] This completes the description of the SASE mechanism for generation of a secure message by an AP. A similar procedure is defined in a later section for decryption of the message at the AVP.

View Gathering

[0501] At the AVP 1106, the Views 1110, 1120 belonging to the same agreement transaction but generated by different AP devices will first be gathered together by the View Gathering Module 1108 before any further authentication and verification processing. When all the views of an agreement are collected, they are given to the Agreement Authentication Module 1118.

[0502] The SAS permits agreement parties to be involved in multiple, simultaneous transactions with differing parties. In addition, multiple transactions from differing parties can also be simultaneously active at the AVP 1106. In general, the view gathering function decides which views belong to the same agreement transaction and at what point the gathering is completed so that all views belonging to the same agreement transaction can be forwarded to the authentication module 1118. A TID must be used to tag each view of an agreement so that the gatherer can match the views belonging to the same agreement and process them together.

[0503] The View Gathering Module 1108 uses the TID in each message to match the views. When the View Gathering Module 1108 has collected the proper number of distinct views, given by NIT, the View Gathering Module 1108 will forward the set of views to the Authentication Module 1118. The parameters TID and NIT are sent in plain text so that the View Gathering Module 1108 can operate on the views prior to authentication and decryption. This permits greater flexibility in that the View Gathering Module 1108 can be physically separated from the AVP 1106. In order to insure the integrity of the TID and NIT, the TID and NIT are repeated in the agreement data. For this purpose, the TID and a list of DIDs of the AP devices involved in the agreement are included in the encrypted portion.

[0504] In alternative implementations, the TID and NIT are only included in the encrypted portion of the message and must be decrypted and authenticated (by the Agreement Authentication Module) prior to handling by the View Gathering Module. In this case, the View Gathering Module holds the decrypted views until a complete set is obtained.

[0505] The View Gathering Module 1108 holds unmatched views of a Transaction for a maximum period of time, called the Transaction Time-out period. After this time has elapsed without collecting a complete set of views, the views are discarded and, optionally, the agreement parties are notified.

Decryption

[0506] The views 1110, 1120 are decrypted at the AVP 1106 by the Agreement Authentication Module (AAM) 1118.

[0507] Figure 60 shows a detailed explanation of the procedure followed by the AAM 1118 and the Agreement Verification Module (AVM) 1112. More particularly, Figure 60 shows a method 1400 of decryption of the above-mentioned AP View 1 1110 and AP View 2 1120, into decrypted AP View1 1410, which includes in plaintext TID, NIT, TS1, DID1, DUID1, and decrypted AP View2 1480, respectively which includes in plaintext TID, NIT, TS2, DID2, DUID2.

[0508] Initially, when the views 1110 or 1120 are received, it is useful for the AAM 1118 to check the validity of the TS of the views. This operation may prevent attacks conducted by changing an AP device clock or replaying an intercepted view. For this purpose, the AVP 1106 stores a clock offset value for each AP device 1101, 1102 in its User and Device Database 1114. This offset describes the difference between the device 1101, 1102's local clock and the system clock of the AVP 1106. With the offset and the TS, the AVP 1106 can verify if the message generated by such a device 1102, 1104 occurs within a reasonable time-window before the message arrives at the AVP 1106. Only messages generated during this period are accepted. Otherwise an "Expired Transaction" error message is generated and sent back to the APs using a method described later in this section. The size of this time window, and the accuracy of the clocks would depend on the requirements set by the application.

[0509] Referring now to Figure 60, when the AAM 1118 is decrypting a transaction view message 1110 from a client 1101, based on the plaintext DID field 1430 of the view 1110 the AAM locates the corresponding pseudorandom sequence number generator R 1434 and seed S for the device 1101 which generated the received view 1110 using the User and Device Database 1114. Then using the TS 1432 also contained in the AP View 1110 as plaintext, the AAM

can inductively reproduce the RSN 1436 which is identical to the RSN 1246 (of Figure 58) used during the derivation of the encryption key. Because the TS value which is required for the AAM to determine the RSN of the view generating AP device 1101, 1102 is enclosed in each message, it is not necessary for the AAM 1118 and the AP devices 1101, 1102 to have synchronized clocks for RSN derivation purposes.

[0510] The AAM 1118 then locates the current user of the AP device 1101 in its User and Device Database 1114 using the DUID field 1433 of the view. By looking into the record for the AP's current user, the AAM 1118 finds the corresponding PIE 1438 of the user. Then the AAM 1118 reconstructs the encryption key 1442 (1250 of Figure 58) used for generating the view 1110 by using the same Hash function 1440 (1245 of Figure 58) used by the AP. With the encryption key known, the AAM can decrypt the full view message contained in the view 1110. After the decryption, if random bit padding was applied during the construction of the view, the padding bits are removed to reveal the true data fields. After the encrypted fields are decrypted, the UID 1422, the DID of the other party 1424, and Data 1426 are fed into a digest algorithm 1446, which is identical to the digest algorithm 1258 used by AP device, to produce a digest 1448. This digest 1448 is then compared with the MD 1428 resulted from decrypting the digital signature contained in the received view. Only if both digests are the same, the digital signature is considered correct. Otherwise, the view is considered altered from the original. The same procedure takes place for the received AP view 1120 in order to ensure that MD2 1478 corresponds to data 1476.

[0511] If the AAM 1118 is not able to successfully decrypt the message or the digital signature is not correct, then the authentication is deemed to have failed. The AP's will be notified through an "Authentication Failed" response message.

[0512] The above described SASE encryption scheme and key generation method is also used by the AVP 1106 to encrypt response messages such as errors or, acknowledgements or receipts that are sent back toAPs 1101, 1102. In general, the response can also contain arbitrary application specific data. For example, it can be used to transmit special tokens generated by the Transaction Processing Component 1116 for AP users for later use.

[0513] Specifically, using the same basic SASE encryption method, to send a response message to AP_I, the AVP will use the destination AP parameter DID_I to determine the random number generator R_I, the $Seed_I$ and a TS determined by the AVP to generate the RSN. Next, the destination APs current user's PIE_I RSN and Hash function are used to generate the encryption key K. A Response Message to AP_I has the following fields and is formatted as:

$$\text{ResponseMessage}_I = \{TID, DID_I, TS, DUID_I, \text{Encryption}[K: (MD, data)]\}.$$

[0514] ResponseMessage, is then transmitted to API. When received, API is able to use the plaintext parameters in the message and its internal parameters to derive the decryption key and decrypt the message. During this process, the AP device may use the included DUID to prompt its user for a PIE if the PIE is not cached at the device.

[0515] In certain situations, because we are using a symmetric cryptography algorithm, in which the same key K derivation procedure can be carried out by either side, the above described AVP response message can be generalized for carrying arbitrary application data in messages.

[0516] When used for sending error messages and receipts back to the APs, the return messages are sent in a reversed path along the Agreement Channels to the APs. If the views are sent separately from each APs (via gathering function) to the AVP, the return messages are also sent independently to the destination APs. Such reverse communication does not need to go through the view gathering module. However, each return message does need to include sufficient information, such as the agreement TID in the message, so that the receiving AP device can identify to which agreement transaction the return message belongs.

Agreement Verification

[0517] After both views 1110, 1120 are successfully decrypted, the AVP 1106 verifies the agreement using the Agreement Verification Module 1112 that executes a procedure consisting of a list of matching rules to be applied to the agreement views. A series of basic matching operations between the fields in the views 1110, 1120 are carried out and then optionally, application specific matching rules can be applied. The basic matching operations are illustrated in Figure 60 and include:

[0518] The DID included in each view's plain text part matches with the DID of the other party included in the other view's encrypted part. That is, 1416 matches with 1474 and 1466 matches with 1424.

[0519] The UID included in each view's cipher text party matches with the current user of the view generating device as determined by the view generating device's device ID and the current user's DUID. That is, the user ID derived from DID_1 1416 and $DUID_1$ 1420 should matches with UID_1 1422 included in the encrypted part of the view. The same matching rule applies to DID_2 1466, $DUID_2$ 1470 and UID_2 1472.

[0520] The Transaction ID, TID 1412 (or 1462), of each view is matched with the TID 1462 (or 1412) of the other

party. In addition, the plaintext NITs are verified by counting the listed DIDs in each view.

[0521] If one of the matching rules is fails during the examination, the verification process is stopped and "Verification Failed" error messages are sent back to both APs using the return message method described earlier. For example, error messages are generated as the following with error1 and error2 being an error code or a descriptive message which both the APs and AVP can understand :

$$\text{ErrorMessage1} = \{\text{TID, DID}_1, \text{TS}_1, \text{DUID}_1, \text{Encryption [K:(MD, error1)] }\}$$

$$\text{ErrorMessage2} = \{\text{TID, DID}_2, \text{TS}_2, \text{DUID}_2, \text{Encryption [K:(MD, error2)] }\}$$

[0522] The next step is for the AVP to verify that the agreement data included in each view's cipher text part matches with each other according to the needs of the application. The SAS is a submission vessel protocol for agreements. Thus it does not define the format and specification of the agreements it carries. Therefore, to accommodate the application in determining whether two agreements really semantically agree with each other, an interface is provided by the AVP so that each application may provide its own additional agreement verification rules for verifying that the agreements included in the views are consistent with each other.

[0523] For example, a simple application independent plug-in procedure that can be used is a bit-matching function. If two agreements are exactly the same, bit by bit, the matching test is passed. More complex plug-ins may involve application specific cryptographic operations and semantic correspondence.

[0524] The Agreement Verification Module 112 may be physically implemented on the AVP, together with the authentication processing implementations. Alternatively, the verification process can be implemented on a different device but able to communicate with the other modules in the AVP through a reliable and secure communication channel.

[0525] At the completion of the verification process, the AVP may forward the agreement data decrypted from received views to a Transaction Processing Component 1116. However, in this case the communication between the AVP 1106 and the Transaction Processing Component carrying out the verification processing must be secure, if not co-located. From the SAS perspective, the agreement data extracted from each received view is already verified by the AVP.

[0526] Because of the additional communication, a timeout mechanism may be included so that if no reply is received from the Transaction Processing Component 1116 process within a certain time, the AVP 1106 sends error messages back to the APs 1101 1102

[0527] When in an application the Transaction Processing Component 1116 is physically located on a different device than the AVP 1106, the application may employ additional cryptography techniques to offer additional privacy features. For example, each AP may apply additional encryption to the agreement data before it applies SAS encryption. This pre-encryption can only be decrypted by the Transaction Processing Component 1116 process, which is not co-located with the AVP. Thus, even the AVP will not be able to discover the contents of the agreement beyond the information needed for basic matching..

[0528] At the end of the verification process, application specific receipts may be generated for theAP's 1101, 1102 describing the result of the verification.

$$\text{ReceiptMessage}_1 = \{\text{TID, DID}_1, \text{TS}_1, \text{DUID}_1, \text{Encryption [K}_1\text{:(MD, receipt}_1\text{)] }\}$$

$$\text{ReceiptMessage}_2 = \{\text{TID, DID}_2, \text{TS}_2, \text{DUID}_2, \text{Encryption [K}_2\text{: (MD, receipt}_2\text{)] }\}$$

[0529] The receipts are sent back to the APs using the method for the AVP to send messages back to APs, as describe earlier. It is important to point out that the contents of the receipts do not need to be understandable by the components of the AVP. This is different from the error messages generated by the authentication process of the AAM. The reason for this distinction is to separate the results from authentication processing from the results from the agreement verification processing. This separation gives the applications more capability to include additional features. For example, when there is an additional Transaction Processing Component 1116 that is physically separated from the AVP, the agreement verification process may include confidential information in its receipts. It is not necessary to allow the AVP to understand the contents of the receipts.

[0530] The departure from the AVP of the receipt or error message for the last AP involved in the agreement marks the end of an agreement authentication and verification transaction at the AVP 1106. The arrival of a receipt at an AP 1101 1102 marks the end of an agreement authentication and verification transaction at the AP.

[0531] AP View 1 1110, AP View 2 1120, and Agreement Verification 1106 are implemented in respective software programs which, when executed by a computer, cause the computer to execute the respective functions described herein above. Each of the programs can be stored on a computer-readable medium.

Extensions of the SAS Protocol

[0532] The above SAS protocol description is presented for agreements between two parties. However, the SAS protocol can be extended for agreements involving more than two parties. In this case, for a transaction involving n parties, the transaction view message from the i-th participant is:

$$ViewMsg_i = \{TID, NIT, DID_i, TS_i, DUID_i, Enc[K_i:(MD_i, TID, UID_i, DID_0, ..., DID_{i-1}, DID_{i+1}, ..., DID_{n-1}, agreement)]\}$$

[0533] Correspondingly, the verification and authentication rules are:

$$ViewMsg_0.DID_i == ... == ViewMsg_j.DID_i == ... == ViewMsg_{n-1}.DID_i, \text{ where } i = 0 ... n-1$$

[0534] For all i's (i)[0, n-1]), using $ViewMsg_i.UID_i$ and $DUID_i$ to search the User and Device Database for the reference UID. This UID should be the same as UID_i included in the encrypted part of the $ViewMsg_i$.

$$ViewMsg_0.TID == ... == ViewMsg_j.TID == ... == VewMsg_{n-1}.TID, \text{ where } i = 0 ... n-1$$

$$ViewMsg_0.NIT == ... == ViewMsg_j.NIT == ... == ViewMsg_{n-1}.NIT, \text{ where } i = 0 ... n-1,$$

and NIT is equal to n, the number of parties listed in the agreement.

[0535] The submission methods of the views in a two AP system are extended to agreement transactions involving more than two APs. If the view gathering and generation processes are separated, exactly the same methods used by a two AP system can be used for a system with more than 2 APs. The View Gathering module collect views from all parties in the agreement using the TID and NIT included in the message.

[0536] When the view gathering function is implemented separately from the view generation function, the view gathering function can be physically implemented at an external device (in which case the APs send their views to this view gathering device then the view gathering device forwards all views together to the AVP.

Alternative View Gathering Methods

[0537] In an alternate version of the invention, called integrated view gathering, the view gathering mechanism is distributed to the APs so that the views are collected sequentially by successive agreement parties as they are transferred to the AVP. If the view gathering and generation are integrated in this manner, a submission chain needs to be set up beforehand among all APs. After the first AP on this chain generates its view, the view is sent to the second AP in this chain. Upon receiving a view from the first AP, the second AP is triggered to generate its own view. Then both views are forwarded to the third AP in this chain, and so on. This process is executed in turn by each AP on this submission chain and finally all views are sent by the last AP on the submission chain to the AVP. In that case, the TID and NIT can be omitted also.

[0538] An example of such an integrated view gathering and generation system is shown in the computer system 1500 of Figure 61. As shown in Figure 61, the first AP device 1502 comprising a local Agreement Channel 1505 generates its view 1522 of the agreement. The view 1522 is sent to the second AP device 1504 via the local agreement channel 1505. Upon receiving the view 1522 from the first AP device 1502, the second AP device generates its view 1524 of the agreement. Then both views 1522 1524 of the agreement are sent to the AVP 1506 via an agreement channel 1503. In some implementations, the views may even be concatenated together and sent as one message. In this variation, because the views are gathered as they are generated, it is no longer necessary for the system 1500 to include a View Gathering component. The AVP 1506 itself comprises three components the Agreement Authentication Module 1510, which is identical to the Agreement Authentication Module 1118, the Agreement Verification Module 1512 which is identical to the Agreement Verification Module 1112, and the User and Device Database 1514, which is identical to the User and Device Database 1114.

[0539] Another variation of the invention permits the assembly of a multi-layered agreement view as a result of an

integrated view gathering architecture. In this system, each successive AP may perform an operation on the agreement data received from APs earlier in the chain. The initial agreement data is included in the view of the first AP. The second AP uses the view received from the first AP as part of its own agreement data and produces its own view, based on a function of the received view. Finally, what the AVP receives is a single, multi-layered view. Combined with the physical separation of AVP modules, such as the AAM and AVM and appropriate encryption/decryption algorithms, applications of this variation can support new capabilities in supporting privacy.

Examples of applications of SAS

[0540] The first application example is shown in Figure 62. It is a wireless payment system 1600 for payments by consumers in physical retail stores. The architecture is similar to that shown in the chained integrated view gathering variation shown in Figure 61. In this example, the backend server called Secure Transaction Sever (STS) 1610 is the AVP. The STS 1610 is further connected to a Transaction Processing Component that is a Financial institution payment serice 1612 to carry out the actual processing of the financial transactions. The APs are the consumers and the merchants and they have their own AP devices 1602 and 1604. For consumers, the AP device 1602 can be any mobile device with wireless capability, such as Personal Digital Assistant, a mobile phone or a credit card sized mini-computing device which are capable of wireless communication and carrying out SAS computations. For merchants, the AP device can be a computer 1604 comprising a wireless LAN access points 1606 providing service to a WLAN service area 1614 and a connection to the backend STS 1610 via the Internet (called an Agreement Channel 1608).

[0541] The agreement is the data requesting a payment transaction between the consumer and the merchant for purchase of physical or virtual goods. After the consumer finalizes her purchase, her AP device 1602 generates her view of the transaction. The view is sent to the merchant device 1604 using a wireless LAN access service, which in turn triggers the merchant device 1604 to generate the merchant's view. Then the merchant device sends both views together to the STS 1610 over the Agreement Channel implemented as a secure Internet connection. After the STS 1610 authenticates the identities of both the merchant and the consumer through decryption, it extracts the monetary transaction request data from the views and performs the basic verification procedures. If successful, the STS forwards the requests to a financial institute 1612 for further transaction processing and eventual monetary exchange. Results from the financial institute 1612 are returned to the STS 1610 and encrypted as receipts to both the merchant and consumer. Both receipts are sent to the merchant device 1604 over the Agreement Channel and the merchant device 1604 forwards the consumer receipt to the consumer device 1602 over the wireless LAN. In a variation, the purchase occurs in two stages, the first stage being a transaction during which the merchant and the consumer request a purchase and the second stage being a transaction during which the consumer and the merchant authorize the purchase, with the consumer also selecting which financial account to use for the transaction.

[0542] In this example, the wireless payment application uses an integrated view gathering approach due to the fact that the consumerAP device 1602 does not have a direct communication link to the AVP 1610 and the merchant device 1604 concatenates its view after it receives a view from client device 1602. At the AVP end, the authentication processing and verification processing are co-located on the STS 1610. In addition to the components, the application also has the additional Transaction Processing Component of a financial institution payment service 1612 to carry out additional application specific processing.

Tokens

[0543] Another application of the SAS is to provide a method of securely distributing special messages called "tokens" that can be thought of as tickets. Such tokens are generated by the AVP as the result of an agreement and sent to one or more members of the agreement. They can be used by members of a previously authenticated agreement to authenticate the other members of the agreement directly without contacting the AVP at the time of authentication. A second use is to authenticate the presentation of the result of a previously authenticated agreement by a third party (who may or may not be a party to the original agreement) without directly contacting the AVP at the time of authentication. The tokens can be used as tickets where in the former case, the identity of the ticket holder and the ticket are important (as in airline tickets), and in the later case, the identity of the ticket holder is not important, just the validity of the ticket. The token should only be used once, as there is not strong security between the two parties.

[0544] Let AP1 and AP2 be two parties of an agreement that has been verified by the AVP. At some time in the future, AP2 would like the ability to verify the identity of AP1 without consulting the AVP again. The token is a type of AVP response message in which the agreement data portion of the response message contains special token identifying information.

[0545] Figure 63 illustrates a method 1800 of using the SAS to generate 3rd-party verifiable tokens.

[0546] As shown in Figure 63, tokens are generated by the AVP in pairs, with one called token 1801 and the other called token receipt 1821. The token 1801 is sent to AP1, the party to be authenticated, while the token receipt 1821

is sent to AP2, the party that wants the authentication service.

[0547] The formats of the token and token receipt are shown in Figure 63. Both are formatted in the same fashion as other AVP response messages. The plaintext part of both token and token receipt contains the same fields as other AVP response messages as described before. Specifically, the plaintext part of token 1801 includes DID1 1802, TS1 1804, DUID1 1806 and the plaintext part of token receipt 1821 includes DID2 1822, TS2 1824 and DUID2 1826. The cipher text part of a token 1801 contains a token identifier TKID 1808 that is used to uniquely identify a token pair, the DID 1810 of AP2, a token code 1812, and other data 1814 associated with the token. The cipher text part of a token 1801 is encrypted by the AVP using a key generated using standard SASE for the current user of AP1. A token receipt 1821 is formatted almost the same as a token except for two differences. The first difference is that the token code 1832 included in the token receipt 1821 is firstly encrypted using SASE with AP1's parameters except for the timestamp. The timestamp could be any future time value TSv chosen by the AVP. Such a TSv 1829 is also included in the cipher text part of the token receipt 1821, which is the second difference between a token and a token receipt.

[0548] Upon receiving a token, AP1, the party whose identity is to be verified, will decrypt the token and store the TKID 1808, DID2 1810, Token Code 1812, and token data 1814 for future use. AP2, the verifying party, stores the TKID 1828, TSv 1829, DID1 1830, token code 1832, and token data 1834. The token code 1832 stored by AP2 is still encrypted by SASE using the parameters for AP1 and TSv. On the other hand, the token code 1812 stored by AP1 is in plaintext form.

[0549] At the time of token verification, AP2 requests that AP1 deliver the token to AP2 by sending a Token Request message containing the TKID 1828 and the TSv 1829 of the token. AP1 receives the request, encrypts the token code 1812 with its own SASE parameters and TSv as timestamp value. Then AP1 transmits the encrypted token code to AP2. At AP2, if the received encrypted token code is found to be the same bit by bit as the locally stored token code 1832, the token is verified and thus the user is authenticated as being a member of the agreement.

[0550] For the second case, where the identity of the token holder is not important, the original token holder can pass the encrypted token to a third party. Let AP1 be the original token holder and AP2 be the verifier. The third party, P, must store the encrypted token and the necessary parameters, such as TKID, TSv, DID2. P presents the token to AP2, by sending an unencrypted message to AP2 containing the TKID, TSv and the token (encrypted by AP1).

[0551] The tokens are useful to verify that a party has a valid result of an agreement. For example, a party has used a mobile computing device to wirelessly purchase movie tickets and has wireless transmitted one ticket to a companion. When the tickets were purchased, a user receives on her device an encrypted token for each ticket and some additional data such as total number of tickets, time, place, etc. The movie theatre also receives the token information. At entry time, each user wirelessly presents one or more tokens and is granted entry.

[0552] The system also includes permanent or removable storage, such as magnetic and optical discs, RAM, ROM, etc. on which the process and data structures of the present invention can be stored and distributed. The processes can also be distributed via, for example, downloading over a network such as the Internet.

[0553] The many features and advantages of the invention are apparent from the detailed specification and, thus, it is intended by the appended claims to cover all such features and advantages of the invention that fall within the true spirit and scope of the invention. Further, since numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation illustrated and described, and accordingly all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.

[0554] In the method of claim 13 the discovery may comprise:

obtaining by the consumer a list of available merchants and contact information to be displayed on his device selecting from the consumer's device the merchant for which a purchase transaction is desired

[0555] In the method of claim 13 the connecting may comprise:

directing by the consumer the consumer device to establish wireless communication using the contact information of the selected merchant; and
accessing by the consumer device the retail application of the merchant device.

[0556] In the method of claim 13 the selecting goods and services may comprise:

providing inputs to the retail application through the consumer device to arrive at the intended list of purchased goods and services from the selected merchant through ordering or other physical means provided by the merchant including scanning,
providing, by the merchant, the accumulated purchase price of the selected goods and services.

[0557] In the method of claim 15, the directing of payment may comprise:

optionally verifying, by the consumer, the merchant with the Secure Transaction Server (STS),
acquiring, by the consumer, the purchase order from the merchant,
optionally verifying, by the consumer, the merchant with the STS,
providing, by the consumer, personal identification information to the consumer device and requesting, by the consumer, a preauthorization by identification information sending a request-transaction (preauthorization) to the STS,
providing, by the merchant, personal identification information to the merchant device and sending a request-transaction to the STS,
responding, by the STS, positively to the consumer and the merchant if the identities and details of the request transaction are verified, and including a listing of accounts to the consumer,
authorizing, by the consumer, the payment to the STS including account selection by an authorization message,
authorizing, by the merchant, the sale to the STS including account selection by an authorization message,
causing, by the STS, the payment from the consumer account to the merchant account if the parties and details of the payment transaction are verified,
responding, by the STS, to the merchant and the consumer with the results of payment transaction.

[0558] In this case, the consumer may combine the request (preauthorization) and authorization as follows:

providing, by the consumer, personal identification information to the consumer device and issuing a request-authorization of the payment to the STS including account selection,
providing, by the merchant, personal identification information to their device and issuing a request-authorization of the sale to the STS including account selection,
causing, by the STS, the payment from the consumer account to the merchant account if the parties and details of the payment transaction are verified,
responding, by the STS, to the merchant and the client with the results of the payment transaction.

[0559] In the method of claim 16, the consumer may combine the request (preauthorization) and authorization as follows:

providing, by the consumer, personal identification information to the consumer device and sending a request-authorization of the payment to the STS including account selection,
providing, by the merchant, personal identification information to the consumer device and issuing a request-authorization of the sale to the STS including account selection,
causing, by the STS, the payment from the consumer account to the merchant account if the parties and details of the payment transaction are verified,
responding, by the STS, to the merchant and the consumer with the results of the payment transaction,
generating, by the merchant, a service token and sending to the consumer representing the payment for service,
sending, by the consumer, an acknowledgement to the merchant containing an encrypted version of the token,
requesting, by the merchant, a token certificate from the STS using the encrypted consumer token,
generating, by the STS, a token certificate and transmitting a copy to the merchant, and
presenting, by the consumer, the token to the merchant upon consumption of the service.

[0560] In the method of claim 16, the consumer may explicitly request a token and combine the authorization and token creation as follows:

providing, by the consumer, personal identification information to the consumer device and creating a request-transaction (preauthorization) to the STS,
providing, by the merchant, personal identification information to the consumer device and creating a request-transaction to the STS,
responding, by the STS, to the preauthorization request-transactions if the identities and details of the request transaction are verified, and including a listing of accounts to the consumer,
sending, by the consumer, a request-token request to the merchant,
generating, by the merchant, a token and sending to the consumer representing the unvalidated payment for service;
sending, by the consumer, a request-authorization-with-token request to the STS containing an encrypted version of the token,
authorizing, by the merchant, the sale by sending a request-authorization-with-token to the STS including account selection,

causing, by the STS, the payment from the consumer account to the merchant account if the parties and details of the payment transaction are verified,
generating, by the STS, a token certificate and transmitting a copy to the merchant, and
presenting, by the consumer, the token to the merchant upon consumption of the service.

[0561] In the method of claim 16, the consumer may use the explicit token request, and combine the preauthorization, authorization and token creation as follows:

creating and sending, by the consumer, a request-token to the merchant,
generating, by the merchant, a token and sending the token by the merchant to the consumer,
the providing, by the consumer, personal identification information to the consumer device and generating a request-authorization-with-token with account selection and containing the encrypted token to the STS,
providing, by the merchant, personal identification information to the merchant device and generating a request-authorization-with-token with account selection to the STS,
causing, by the STS, the payment from the consumer account to the merchant account if the parties and details of the payment transaction are verified,
creating, by the STS, a token certificate for representing the payment for the service,
responding, by the STS, to the consumer with a message containing the results of the payment transaction, and
responding, by the STS, to the merchant with a message containing the results of the payment transaction and the token certificate,
the consumer presenting the token to the merchant upon consumption of the service.

[0562] In the method of claim 16. the consumer may combine the preauthorization, authorization and token creation as follows:

providing, by the consumer, personal identification information to their device and generating a request-authorization-token with account selection to the STS,
providing, by the merchant, personal identification information to their device and generating a request-authorization-token with account selection to the STS,
causing, by the STS, the payment from the consumer account to the merchant account if the parties and details of the payment transaction are verified,
creating, by the STS, a service token and corresponding token certificate for representing the payment for the service,
responding, by the STS, to the merchant with a message including the results of the payment transaction and the token certificate, and
responding, by the STS, to the consumer with a message including the results of the payment transaction and the token,
the consumer presenting the token to the merchant upon consumption of the service.

[0563] In the method of claim 16, the consumer may present the token and be validated by the merchant as follows:

encrypting, by the consumer device, a service token, creating a token certificate, and submitting the token certificate to merchant,
determining, by the merchant device, if a valid copy of the token certificate has been previously stored and not used, if valid then the service is provided and token certificate deleted from merchant storage.

[0564] In the method of claim 16, the consumer may present the token and be validated by the merchant and the STS comprising:

encrypting, by the consumer device, a service token, creating a token certificate, and submitting the token certificate to the STS,
determining, by the STS, whether a valid copy of token certificate has been previously stored and not used, if valid then marking the token certificate as used and providing a response to the merchant,
providing, by the merchant, a service to the consumer

[0565] In the method claim 16, presenting the token to the merchant may comprise:

converting, by the consumer device, the token to a barcode and displaying the token represented as a barcode

on its display, and

scanning, by the merchant device, the barcode, converting the barcode to a token and then checking the token.

[0566] In the computer system of claim 25, the mobile consumer device may be packaged as a credit card-sized device (approximately 55mm x 85 mm) and approximately 10mm thick or thinner.

[0567] In the computer system of claim 25, the wireless network interface of the mobile consumer device can be any of, WiFi, Bluetooth, UWB, IR, Zigbee, or other local wireless network interface, or a cellular telephone network.

[0568] The wireless network that the mobile consumer device is capable of connecting to, may include a cellular telephone network and the consumer device may include proximity binding such as a barcode display, a barcode an RF-ID tag or location determination.

[0569] The consumer device may be capable of binding to a physical goods purchase or token presentation using a device such as a barcode display, a barcode an RF-ID tag or location determination.

[0570] The mobile consumer device may include means for indicating readiness to authorize payment such as a "Pay" button or a touch screen "Pay" button.

[0571] In the computer system of claim 25, the mobile consumer device may have no display, and may comprise means for communicating output including synthesized speech.

[0572] In the computer system of claim 25, the mobile consumer device may have no buttons or touch screen and may include a microphone and may be capable of processing input by speech recognition.

[0573] In the computer system of claim 25, the mobile consumer device may further comprise a biometric sensor for user identification such as fingerprint or face recognition.

[0574] In the computer system of claim 25, the mobile consumer device may interface to a display located remotely from the consumer device, on the merchant device.

[0575] In the computer system of claim 25, the mobile consumer device may be a Personal Digital Assistant (PDA) or a mobile phone.

[0576] In the computer system of in claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface including WIFI and an access point operated by the merchant device and the merchant device providing a directory service on the wireless network.

[0577] In the computer system of claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface including IR and an access point operated by the merchant device.

[0578] In the computer system of claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface including UWB and an access point operated by the merchant device.

[0579] In the computer system of claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface including Zigbee and an access point operated by the merchant device.

[0580] In the computer system of claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface including WIFI and one or more access points operated by another party as a hotspot application.

[0581] In the computer system of claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface including Bluetooth and one or more access points operated by another party as a hotspot application.

[0582] In the computer system of claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface including IR and one or more access points operated by another party as a hotspot application.

[0583] In the computer system of claim 24, the wireless network interface may comprise a local wireless interface including UWB and one or more access points operated by another party as a hotspot application.

[0584] In the computer system of claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface including Zigbee and one or more access points operated by another party as a hotspot application.

[0585] In the computer system of claim 24, the wireless network interface of the mobile consumer device may comprise a local wireless interface as a point-to-point connection based on IR.

[0586] In the computer system of claim 24, wherein the wireless network interface of the mobile consumer device may comprise a cellular phone interface and proximity binding of the consumer.

[0587] In each of the cases set out above, the local wireless network may comprise multiple access points operated by the merchant.

[0588] Alternatively in each of the cases set out above the local wireless network may comprise multiple access points operated by another party but granting access to merchants and consumers.

[0589] In the system of claim 50, the operator of the trusted secure transaction server may collect a fee for processing a transaction from one or more of the consumer, merchant, payment services, credit card issuers and financial accounts based on a fee for each transaction or on a percentage of transaction amount.

[0590] The system of claim 50 may further comprise a secure network coupling the merchant operated device with the trusted secure transaction server, and the wireless local area network may be operated by the merchant operated device.

[0591] The system of claim 50 may further comprise a secure network coupling the merchant operated device with the trusted secure transaction server, and the wireless local area network may include a hotspot accessible by a plurality of merchants and consumers and at which the consumer can select and access the merchant through the wireless local area network.

[0592] In the system of claim 50, the wireless local area network may include a hotspot accessible by a plurality of merchants and consumers and at which the consumer can select and access the merchant through the wireless local area network and a directory.

[0593] In the system of claim 50, the wireless local area network may include a hotspot accessible by a plurality of merchants and consumers and at which the consumer can select and access the merchant through the wireless local area network, and the merchant device, the consumer device, and the trusted secure transaction server may be in communication with each other via the hotspot.

[0594] In the system of claim 50, the merchant device may execute a retail application and a secure transaction purchasing application, can execute the secure transaction application on a local device at the merchant location connected to the wireless local area network and a remote device connected via another network to the wireless local area network and the consumer device.

[0595] In each of the cases set out above, the merchant device may be connected to the trusted secure transaction server via the Internet using additional security including but not limited to the secure socket layer (SSL) or a Virtual Private Network.

[0596] Alternatively, in each of the cases set out above, the trusted secure transaction server may be connected to one or more payment services through a secure network or through the Internet using additional security including but not limited to the secure socket layer (SSL) or a Virtual Private Network.

[0597] In the system of claim 50 a consumer can request that the Secure Transaction Server disable the device and thereby not permitting further transactions for that device with the current personal identification information.

[0598] In the system of claim 50 the Secure Transaction Server can detect and disable a consumer account if there are multiple attempts to authorize a payment with incorrect personal identifying information.

[0599] In the system of claim 50, the consumer can purchase a service, including a movie ticket, from the merchant using a mobile device; receive an electronic token as proof of payment; and the consumer can present the token to obtain the service using their mobile device, including a paperless e-ticket.

[0600] In the system of claim 50 the transaction may be a return of goods and services from the consumer to the merchant and the secure transaction server may cause payment from the merchant to the consumer.

[0601] In the system of claim 50 the Secure Transaction Server may provide ancillary information from the payment services, including but not limited to, advertisements, special interest rate for a particular purchase if a specific credit account is chosen for the attempted purchase, to the consumer in the response messages prior to the final purchasing authorization by the consumer.

[0602] This application claims priority from U.S. Provisional Application Serial Number 60/401,807, Attorney Docket No. 1634.1002P, entitled METHODS AND APPARATUSES FOR SECURE MULTI-PARTY FINANCIAL TRANSACTIONS (A UNIVERSAL PERVASIVE TRANSACTION FRAMEWORK), by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed August 8, 2002 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference. also claims priority from U.S. Patent Application No.

[0603] This application also claims priority from U.S. Patent Application No._____ Attorney Docket No. 1634.1002, entitled METHODS FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0604] This application also claims priority from U.S. Serial Number 10/458,205, Attorney Docket No. 1634.1003, entitled SECURITY FRAMEWORK AND PROTOCOL FOR UNIVERSAL PERVASIVE TRANSACTIONS, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed June 11, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference. European patent application no. , Attorney Docket No. HL 85760/PMH, filed on the same date as the present application, corresponds to US 10/458,205, and the contents of this European application are also incorporated herein by reference.

[0605] This application also claims priority from U.S. Patent Application No. Attorney Docket No. 1634.1004, entitled APPARATUSES FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

[0606] This application also claims priority from U.S. Patent Application No. Attorney Docket No. 1634.1005, entitled FRAMEWORK AND SYSTEM FOR PURCHASING OF GOODS AND SERVICES, by Yannis Labrou, Lusheng Ji, and

Jonathan Agre, filed July 29, 2003 in the U.S. Patent and Trademark Office, the contents of which are incorporated herein by reference.

Claims

1. A method for conducting a purchasing agreement for goods and services between a consumer and a merchant through a trusted a third party and using a wireless network comprising:

   generating, by the consumer, a first view of the agreement and transmitting the first view of the agreement to the third party;
   generating, independently by the merchant, a second view of the agreement and transmitting the second view of the agreement to the third party; and
   receiving, by the third party, comprising a Secure Transaction Server, the consumer view of the agreement and the merchant view of the agreement, verifying identities of the merchant and the consumer and that the details of the independently generated views of the agreements are consistent and taking action to execute the purchasing agreement if the conditions are satisfied.

2. The method of claim 1, wherein the purchasing agreement includes the ordering of and paying for goods or services.

3. The method of claim 2, further comprising conducting purchases using local wireless communication between a consumer operated mobile device and a merchant operated device and a Secure transaction Server device, comprising the trusted third party, and parts of the messages communicated between the devices and the secure transaction server are encrypted using the Secure Transaction Protocol.

4. The method as in claim 3, wherein the trusted third party returns a token as receipt of payment that is presented by the consumer to the merchant to obtain the paid-for services at a later time.

5. The method as in claim 4 for a consumer to conduct a purchase transaction with a merchant using a consumer operated mobile device in wireless local communication with a merchant device, comprising:

   discovering, by the consumer device, the merchant device via the network;
   connecting, by the consumer device, to the merchant device via the network;
   selecting, by the consumer using the consumer device, the goods and services to be purchased;
   obtaining a purchase order from the merchant containing the transaction details such as amount and authorizing by the consumer using the consumer device, payment to the merchant for the goods and services through the secure transaction server.

6. The method of claim 5, wherein the discovering comprising automatically scanning the wireless network or manually discovering one or more merchant devices and the consumer then selecting one of the merchant devices from a list of merchant devices presented by the consumer device.

7. The method of claim 6, wherein the connecting comprising connecting the consumer device to the selected merchant device through the wireless local communication network.

8. The method of claim 7, wherein the selecting comprising selecting one of the goods or services from a list of the goods and services of the merchant presented by the consumer device.

9. The method of claim 8, further comprising:

   transmitting by the consumer device a request for a purchase order for items to be purchased to the merchant device;
   preparing by the merchant device a purchase order with information including pricing and transmitting the purchase order to the consumer device; and
   upon receiving the purchase order by the consumer device, authorizing by the consumer device payment for the purchase order.

10. The method of claim 9, further comprising verifying the merchant device by the secure transaction server before

the purchase order is transmitted to the consumer device.

11. The method of claim 10, further comprising verifying the merchant device by the secure transaction server after the purchase order is transmitted to the consumer device.

12. The method of claim 11, further comprising:

indicating, by the consumer, intent to proceed with payment for the purchase order via a command entered into the consumer device;
upon receiving the command and a positive result of merchant verification by the secure transaction server, the consumer device indicating the intent to authorize payment and transmitting the intent to the secure transaction server via the merchant; and
upon receiving a positive result of the verification by the secure transaction server, the merchant indicating the intent to authorize acceptance of payment and transmitting the consumer intent and the merchant intent to the secure transaction server.

13. The method of claim 12, further comprising:

upon receiving the authorization for payment from the consumer and authorization for acceptance from the merchant, interacting by the secure transaction server with a payment service to cause the transfer of funds or commitment for transfer of funds from the consumer to the merchant to occur; and
upon completion of the transfer of funds, transmitting by the secure transaction server, a confirmation to the consumer and the merchant.

14. The method of claim 13 wherein the purchase is for services (and certain goods) and the Secure Transaction Server causes a token to be sent to the consumer and the merchant as proof of payment and that can be presented when the service is activated or consumed, or goods received.

15. The method of claim 13 wherein the transaction comprises the purchase of physical goods.

16. The method as in claim 14 wherein the direction of payment comprising:

optionally verifying, by the consumer, the merchant with the STS,
acquiring, by the consumer, the purchase order from the merchant,
optionally verifying, by the consumer, the merchant with the STS,
providing, by the consumer, personal identification information to the consumer device and sending a request-transaction (preauthorization) to the STS,
providing, by the merchant, personal identification information to the merchant device and sending a request-transaction to the STS,
responding, by the STS, to the preauthorization request-transactions if the identities and details of the request transaction are verified, and including a listing of accounts to the consumer,
sending, by the consumer sending an authorization for the payment to the STS including account selection,
authorizing, by the merchant, the sale to the STS including account selection,
causing, by the STS, the payment from the consumer account to the merchant account if the parties and details of the payment transaction are verified,
responding, by the STS, to the merchant and the consumer with the results of the payment transaction,
generating, by the merchant, a service token and sending to the consumer representing the payment for service,
sending, by the consumer, an acknowledgement to the merchant containing an encrypted version of the token,
requesting, by the merchant, a token certificate from the STS using the encrypted consumer token,
generating, by the STS, a token certificate and transmitting a copy to the merchant, and
presenting, by the consumer, the token to the merchant upon consumption of the service.

17. The method as in any one of claims 14, 15 and 16, wherein the consumer acquiring the purchase order includes implicit verification of the merchant identity by the STS and comprising:

transmitting, by the consumer device, a request for a purchase order for the items to be purchased to the merchant device,

preparing, by the merchant device, a purchase order with relevant information such as pricing,
transmitting, by the merchant device, the purchase order (PO) to the STS,
verifying, by the STS, the merchant identity and creating an STS version of the PO from the merchant PO (STS-PO), and
transmitting, by the STS, the STS-PO to the merchant the merchant transmits the STS-PO to the consumer device, so that upon receipt of the STS-PO the consumer has positive verification that the merchant is a registered UPTF merchant.

18. The method as in any one of claims 14, 15 and 16, wherein the verifying the merchant comprising:

obtaining, by the consumer, the merchant legal name and address from a merchant device advertisement, or a directory service,
issuing, by the client, a merchant verification transaction including the merchant information and merchant device identifier and sending the merchant verification transaction to the merchant device,
forwarding, by the merchant device, to the STS the merchant information and the merchant device identity,
verifying, by the STS, the merchant information and the merchant device identity with its records,
returning, by the STS, a merchant verification response message to the merchant for forwarding to the consumer,
receiving, by the consumer, the message indicating whether the merchant is valid.

19. The method as in any one of claims 14, 15 and 16 wherein the consumer acquiring the purchase order comprising:

sending, by the consumer, an explicit generate-purchase-order to the merchant,
creating, by the merchant, a purchase order corresponding to the items selected by the consumer and sending the purchase order to the consumer.

20. A computer system for conducting purchase transactions using wireless communication between a consumer and a merchant, comprising:

a consumer operated mobile device;
a merchant operated device;
a trusted secure transaction server (STS) device;
one or more payment service devices;
a wireless communication network in communication with the consumer device and the merchant device;
a communication network in communication with the merchant device and the STS device;
a communication network in communication with the STS device and the payment service devices,
wherein the consumer device, merchant device and secure transaction server device are capable of executing the Secure Transaction Protocol.

21. The computer system as in claim 20, wherein the wireless network is a local wireless network and consumer device is in proximity to the merchant device.

22. The computer system as in claim 21, wherein the consumer device allows the consumer to input identification information into consumer device.

23. The computer system as in claim 22 wherein the consumer device is mobile device, coupled to a wireless network and comprising:

a wireless network interface connecting to the wireless network,
a processor executing a web browser application, purchasing application executing the Secure Transaction Protocol and a submit receipt application.

24. The computer system as in claim 21 wherein the merchant device is coupled to a wireless network for communication with a consumer and a wired or wireless network for communication to the STS and comprising:

a wireless network interface connecting to the wireless network for the consumer,
a wired or wireless network interface connecting to the wireless network for the STS,
a processor executing a merchant retail application program and a purchasing application program executing

the Secure Transaction Protocol (STP).

25. The computer system as in claim 23, wherein the mobile consumer device is packaged as a portable device, comprising:

a lightweight processor with storage capable of executing the Secure Transaction Protocol (STP) and a web browser application;
a wireless network interface and connection to a wireless network, and capable of connecting to a merchant device;
a battery;
a display for communicating output to a user and for other interaction with its user, and
means for user to input information, including navigation buttons or touch screen.

26. The computer system of claim 25, wherein the merchant device interfacing to a consumer device through the wireless network and executing a physical goods purchase and binding a consumer device to the physical goods purchase.

27. The computer system as in claim 26 further comprising partitioning in which the merchant retail application program and the universal pervasive transaction framework application program are executed in separate partitions of the merchant device.

28. The computer system as in claim 27, further comprising a secure network connection to a secure transaction server.

29. The computer system as in claim 28, wherein the secure network connection to the secure transaction server is the Internet.

30. The computer system as in claim 28, wherein the secure network connection to the secure transaction server is wireless.

31. The computer system of any one of claims 20 to 30 in which the secure transaction server is operated in a secure physical environment so that the integrity of the consumer and merchant accounts is protected.

32. The computer system of claim 31 further comprising a multiple server system to handle geographic and temporal differences in demand, and preserving the behavior and security properties of the Secure Transaction Protocol.

33. A system for conducting an agreement between two parties relying on a trusted a third party comprising:

a first party generating a first view of the agreement and transmitting the first view of the agreement to the third party;
a second party independently generating a second view of the agreement and transmitting the second view of the agreement to the third party;
a wireless network connecting the first party and the second party, and
a wired or wireless network connecting the second party to the third party; wherein the trusted third party, receiving the first view of the agreement and the second view of the agreement, verifying conditions including that the identities of the parties that transmitted the agreements and that the independent views of the agreement are consistent with each other and takes action to execute the agreement if the conditions are satisfied.

34. A system as in Claim 33 wherein the agreement pertains to the ordering and or purchasing of goods and services, the first party is a consumer, the second party is a merchant and the third party is a Secure Transaction Server entity.

35. A system as in Claim 34 wherein the generation of views by each party and the verification procedure is based on a secure, symmetric agreement verification protocol.

36. A system as in claim 35 wherein the secure, symmetric agreement verification protocol is the Secure Transaction Protocol.

37. A system of claim 36, further comprising one or more payment service devices and wherein:

the first party comprises a consumer operating a mobile device with an associated identification number;
the second party comprises a merchant operating a device with an associated identification number;
the third party operating a trusted secure transaction server device;
the wireless communication network is in communication with the consumer device and the merchant device;
the wired or wireless communication network is in communication with the merchant device and the trusted secure transaction server device,
and wherein the consumer device, the merchant device, and the trusted secure transaction server device are capable of executing the Secure Transaction Protocol.

38. A system as Claim 36, where the consumer is connected to the merchant via a wireless local area network.

39. The system as in claim 38, wherein the consumer and the merchant do not trust each other and the wireless local area network is open and not secure and the secure transaction server is able to verify the identity of the agreement parties and purchase agreement details.

40. The system as in claim 39 wherein the mobile device stores no personal identifying information about the consumer or account information of the consumer and such account information of the merchant and the consumer is stored in the trusted secure transaction server or is accessible by the secure transaction server.

41. The system as in claim 40, further comprising one or more payment services which execute a payment upon direction of the trusted secure transaction server, wherein the trusted secure transaction server is in secure communication with one or more payment services, including online payment services, financial institutions, and credit card agencies, using a wired or wireless network and the trusted secure transaction server directs that payment be executed by the payment services upon validation of the purchase transaction by the trusted secure transaction server.

42. The system as in claim 41, wherein consumer identifying information and merchant identifying information is stored only in the trusted secure transaction server, and, for authorization by the trusted secure transaction server, the merchant enters merchant identifying information into the merchant device and the consumer enters consumer identifying information into the consumer device.

43. The system as in claim 42, wherein the purchase transaction is for goods and services and the trusted secure transaction server supplies a token as confirmation of payment.

44. The system as in claim 43, wherein the consumer presents the token to the merchant in order to consume a service.

45. The system as in claim 44, wherein only the trusted secure transaction server, and neither the merchant nor the consumer are able to observe details of the other's transaction or identity information.

46. The system as in claim 45, wherein the consumer may be required to authenticate himself to the consumer device, prior to using the device, by entering a personal identifying information, including but not limited to a PIN, password, or by providing biometric authentication, including, but not limited to a fingerprint or a voiceprint.

47. The system as in claim 46, wherein the consumer only authorizes payment through an explicit command to their device, by entering a personal identifying information, including but not limited to a PIN, password, or by providing biometric authentication, including, a fingerprint or a voiceprint.

48. The system as in claim 47, wherein the consumer can select from among financial accounts of the consumer from information stored at the trusted secure transaction server or accessible by the secure transaction server, in order to use the selected account for payment.

49. The system as in claim 48, wherein the consumer and the merchant execute a registration process with the trusted third party by securely providing account information to the trusted secure transaction server and obtaining software to execute the Secure Transaction Protocol, and said registration procedure occurring prior to executing a purchasing transaction and said registration procedure includes providing account information and a unique identifier of the respective consumer operated device or merchant operated device and receive from the trusted secure transaction server device a personal identifying information, such as a PIN, to be only used with the respective consumer operated device or merchant operated device.

50. A system as in claim 49 wherein the conducting of purchase agreements, comprises:

discovering the merchant device by the consumer operating the mobile device; selecting, by the consumer, goods or services to purchase;
obtaining, from the merchant device, a purchase order;
authorizing, by the consumer, the payment for the purchase order through the consumer device;
authorizing, by the merchant through the merchant device, acceptance of the payment; verifying by a trusted secure transaction server, identities of the merchant and the consumer and details of the transaction;
causing, by the trusted secure transaction server, payment from the consumer to the merchant through a payment service; and
issuing, by the trusted secure transaction server, receipts to the consumer device and to the merchant device indicating success or failure of the transaction.

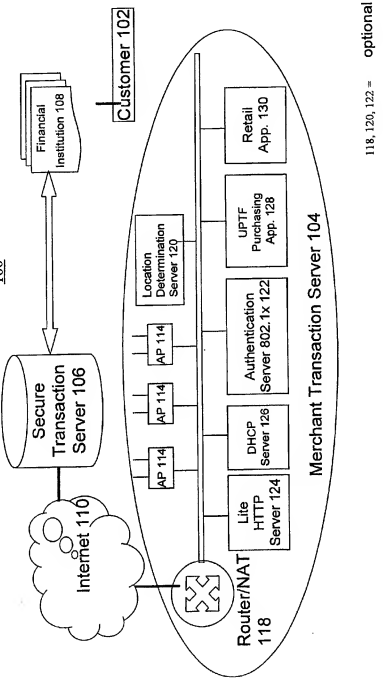

100
Financial Institution 108
Customer 102
Secure Transaction Server 106
Internet 110
Router/NAT 118
Merchant Transaction Server 104
AP 114
AP 114
AP 114
Lite HTTP Server 124
DHCP Server 126
Authentication Server 802.1x 122
Location Determination Server 120
UPTF Purchasing App. 128
Retail App. 130
118, 120, 122 = optional

Figure 1

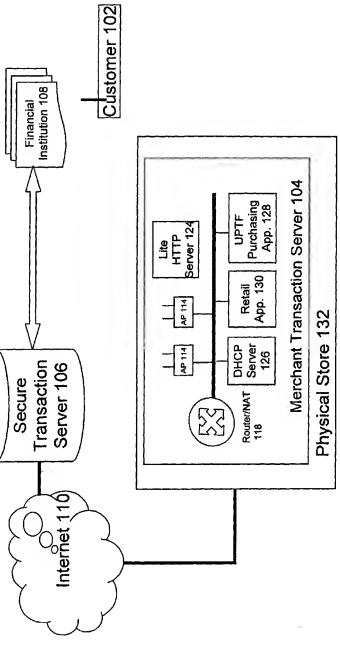

Customer 102
Financial Institution 108
Secure Transaction Server 106
Internet 110
Physical Store 132
Merchant Transaction Server 104
Router/NAT 118
DHCP Server 126
AP 114
AP 114
Retail App. 130
Lite HTTP Server 124
UPTF Purchasing App. 128

Figure 2

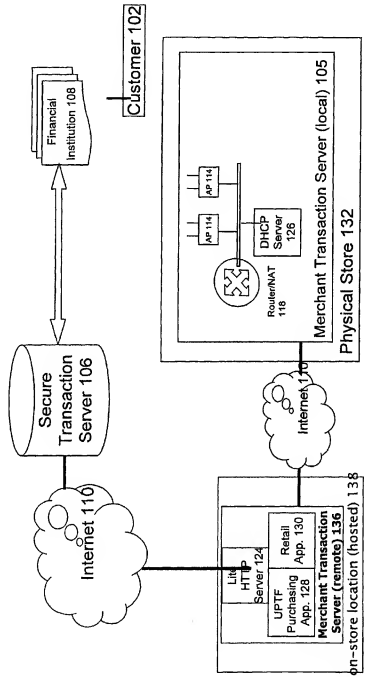

Financial Institution 108
Customer 102
Secure Transaction Server 106
Internet 110
Internet 104
Merchant Transaction Server (local) 105
Physical Store 132
AP 114
AP 114
DHCP Server 126
Router/NAT 116
Lite HTTP Server 124
UPTF Purchasing App. 128
Retail App. 130
Merchant Transaction Server (remote) 136
On-store location (hosted) 138

Figure 3

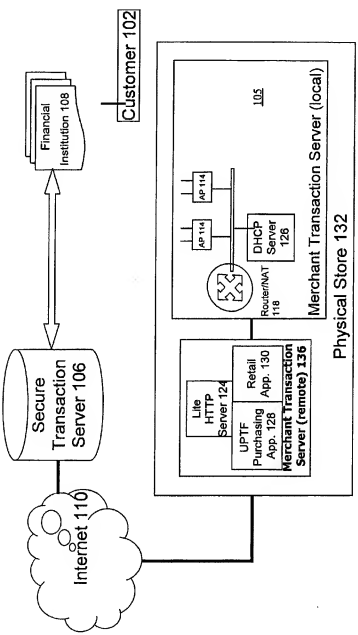

Customer 102
Financial Institution 108
Secure Transaction Server 106
Internet 110
Physical Store 132
Merchant Transaction Server (local)
105
AP 114
AP 114
DHCP Server 126
Router/NAT 118
Lite HTTP Server 124
UPTF Purchasing App. 128
Retail App. 130
Merchant Transaction Server (remote) 136

Figure 4

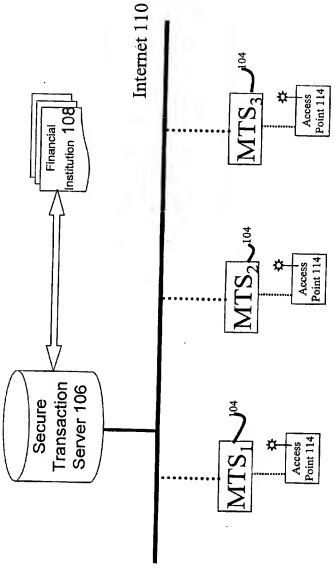

Internet 110
Financial Institution 108
Secure Transaction Server 106
MTS1 104
MTS2 104
MTS3 104
Access Point 114
Access Point 114
Access Point 114
Customer 102

Figure 5

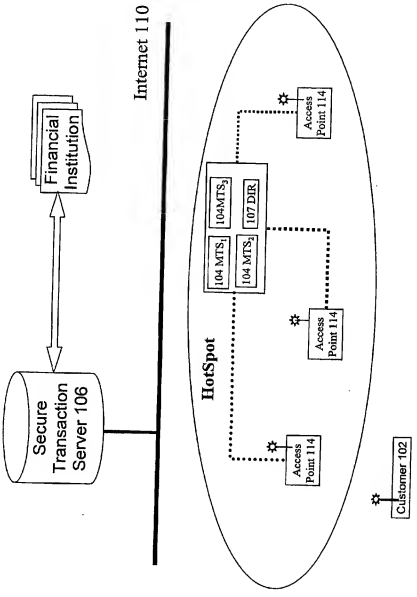

Financial Institution
Internet 110
Secure Transaction Server 106
HotSpot
104 MTS1
104 MTS2
104MTSn
107 DIR
Access Point 114
Access Point 114
Access Point 114
Customer 102

Figure 6

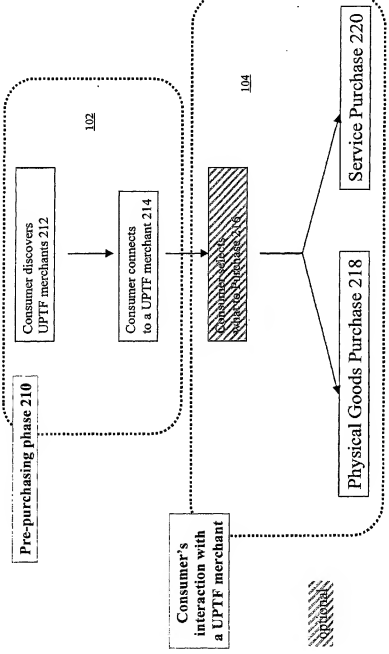

200
Pre-purchasing phase 210
Consumer discovers UPTF merchants 212
102
Consumer connects to a UPTF merchant 214
104
Consumer's interaction with a UPTF merchant
optional
Physical Goods Purchase 218
Service Purchase 220

Figure 7

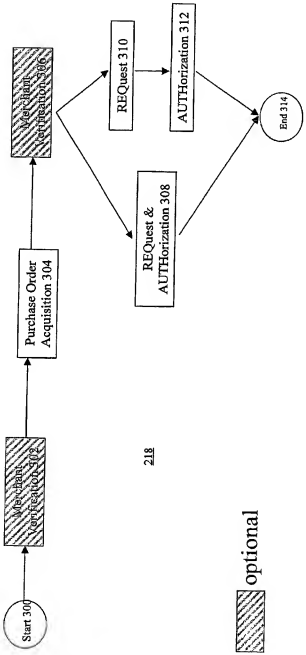

Start 300
Merchant Certification 302
Purchase Order Acquisition 304
Merchant Certification 306
REQuest & AUTHorization 308
REQuest 310
AUTHorization 312
End 314
218
optional

Figure 8

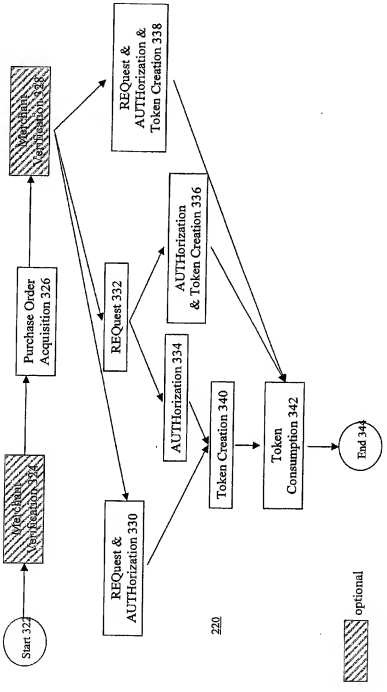

Start 322
Wallet Initialization/Personalization 324
Purchase Order Acquisition 326
Merchant Verification 328
REQuest & AUTHorization 330
REQuest 332
AUTHorization 334
Token Creation 340
Token Consumption 342
End 344
AUTHorization & Token Creation 336
REQuest & AUTHorization & Token Creation 338
220
optional

Figure 9

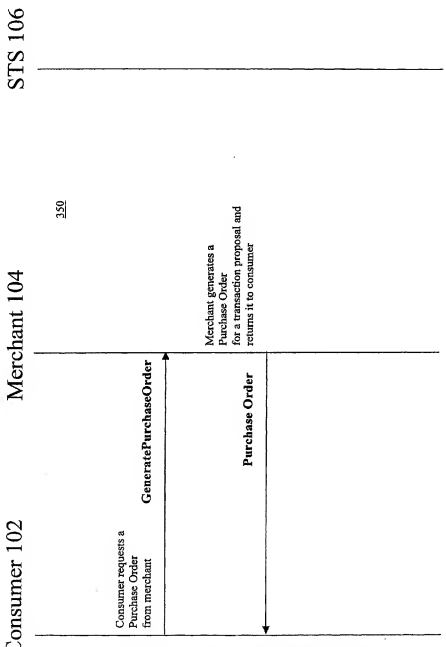


Figure 10

Purchase Order Acquisition - Direct Purchase Order Exchange

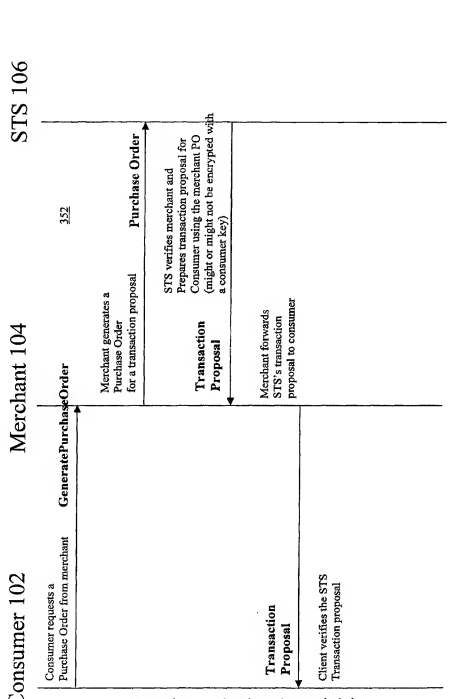

Consumer 102
Merchant 104
STS 106
Consumer requests a Purchase Order from merchant
GeneratePurchaseOrder
Merchant generates a Purchase Order for a transaction proposal
352
Purchase Order
STS verifies merchant and Prepares transaction proposal for Consumer using the merchant PO (might or might not be encrypted with a consumer key)
Transaction Proposal
Merchant forwards STS's transaction proposal to consumer
Transaction Proposal
Client verifies the STS Transaction proposal
Purchase Order Acquisition – Purchase Order Request

Figure 11

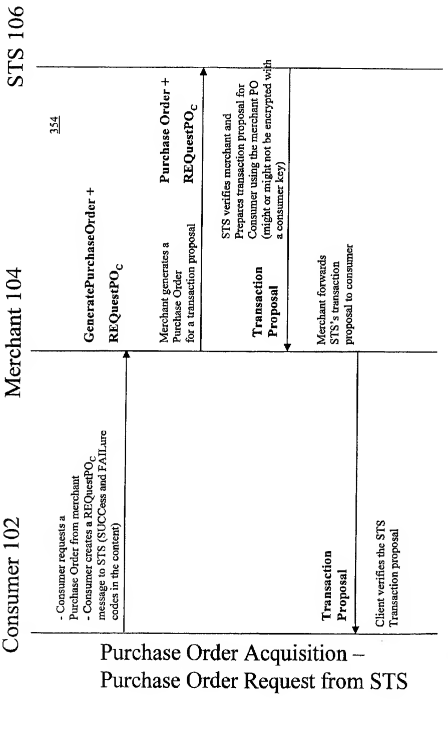
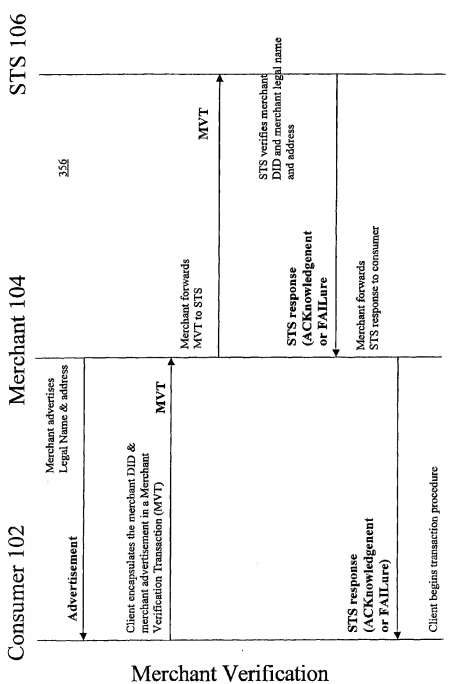

Consumer 102
Merchant 104
STS 106
354
- Consumer requests a Purchase Order from merchant
- Consumer creates a REQuestPO$_C$ message to STS (SUCCess and FAILure codes in the content)
GeneratePurchaseOrder +
REQuestPO$_C$
Merchant generates a Purchase Order for a transaction proposal
Purchase Order +
REQuestPO$_C$
STS verifies merchant and Prepares transaction proposal for Consumer using the merchant PO (might or might not be encrypted with a consumer key)
Transaction Proposal
Merchant forwards STS's transaction proposal to consumer
Transaction Proposal
Client verifies the STS Transaction proposal
Purchase Order Acquisition –
Purchase Order Request from STS

Figure 12



Merchant Verification

Figure 13

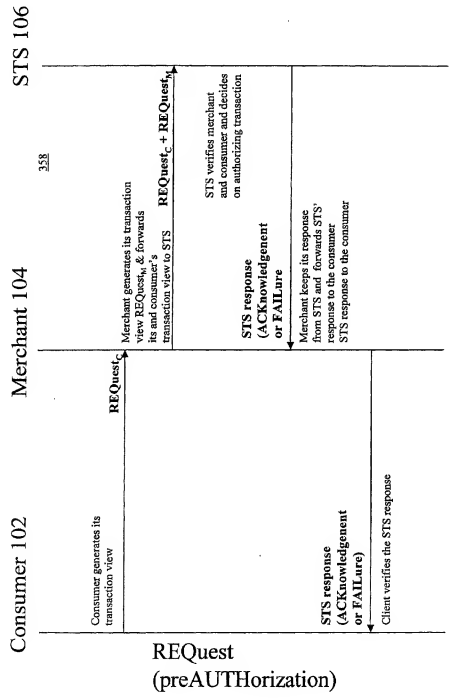

Consumer 102
Merchant 104
358
STS 106
Consumer generates its transaction view
REQUest$_C$
Merchant generates its transaction view REQuest$_M$ & forwards its and consumer's transaction view to STS
REQUest$_C$ + REQUest$_M$
STS verifies merchant and consumer and decides on authorizing transaction
STS response (ACKnowledgement or FAILure
Merchant keeps its response from STS and forwards STS' response to the consumer
STS response (ACKnowledgement or FAILure)
STS response to the consumer
Client verifies the STS response
REQUest (preAUTHorization)

Figure 14

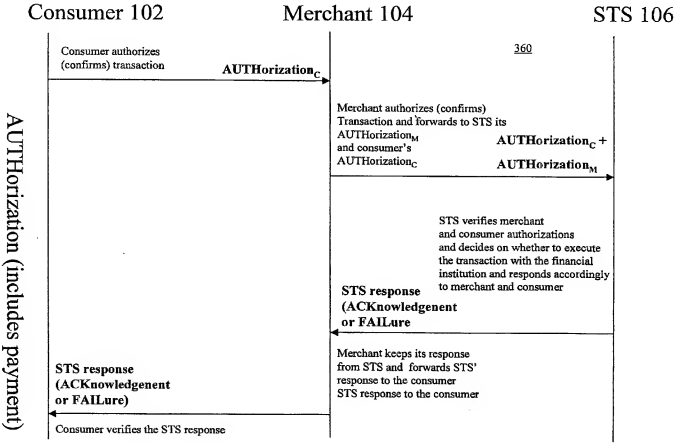
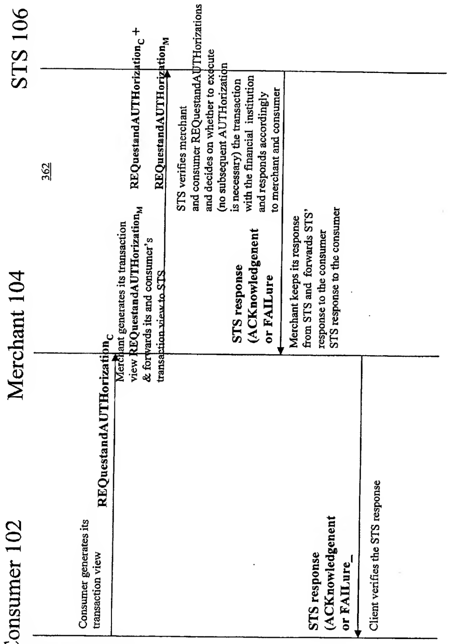
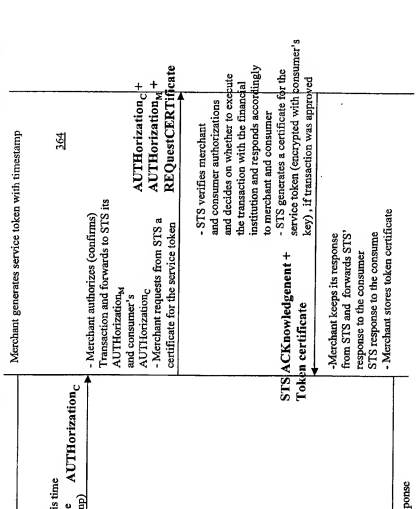

Consumer 102
Merchant 104
STS 106
AUTHorization (includes payment)
Consumer authorizes (confirms) transaction
AUTHorization$_C$
360
Merchant authorizes (confirms) Transaction and forwards to STS its AUTHorization$_M$ and consumer's AUTHorization$_C$
AUTHorization$_C$ + AUTHorization$_M$
STS verifies merchant and consumer authorizations and decides on whether to execute the transaction with the financial institution and responds accordingly to merchant and consumer
STS response (ACKnowledgenent or FAILure
Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consumer
STS response (ACKnowledgenent or FAILure)
Consumer verifies the STS response

Figure 15



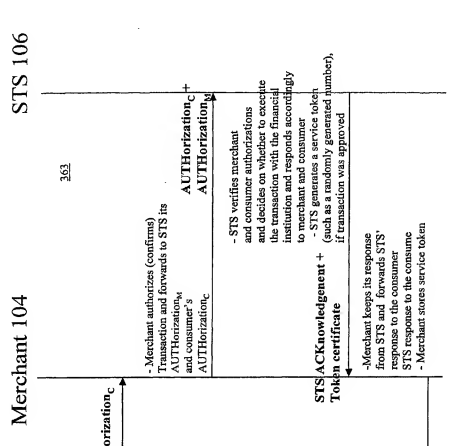
Single step
REQuest and AUTHorization (includes payment)

Figure 16



Token Creation and AUTHorization

Figure 17



Token Creation and AUTHorization

Figure 18

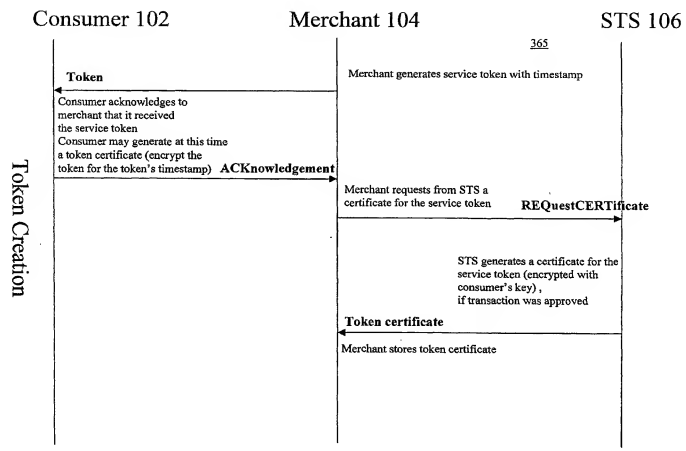
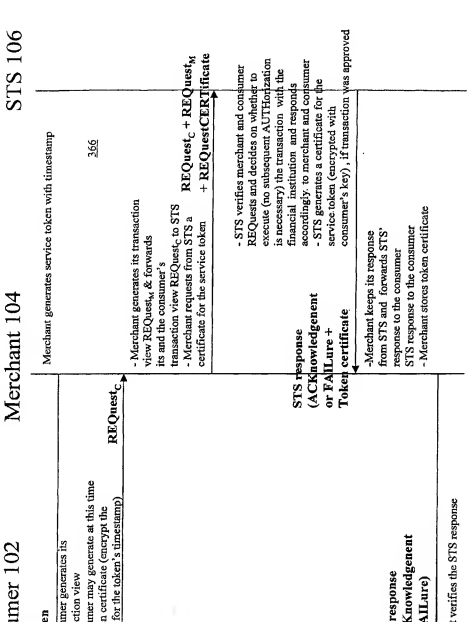

Consumer 102
Merchant 104
STS 106
365
Token
Merchant generates service token with timestamp
Consumer acknowledges to merchant that it received the service token
Consumer may generate at this time a token certificate (encrypt the token for the token's timestamp)
ACKnowledgement
Merchant requests from STS a certificate for the service token
REQuestCERTificate
STS generates a certificate for the service token (encrypted with consumer's key), if transaction was approved
Token certificate
Merchant stores token certificate
Token Creation

Figure 19



Single step REQuest, AUTHorization and Token Creation

Figure 20

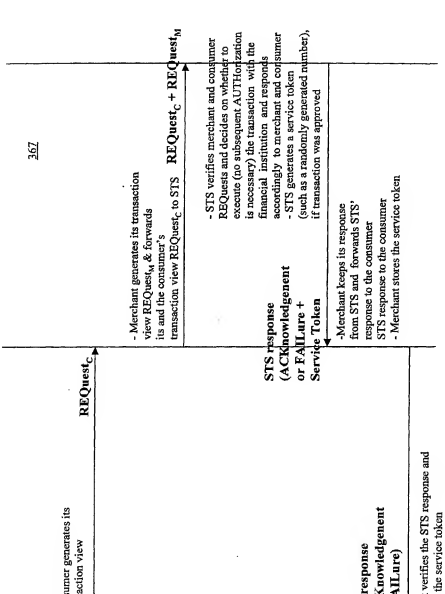
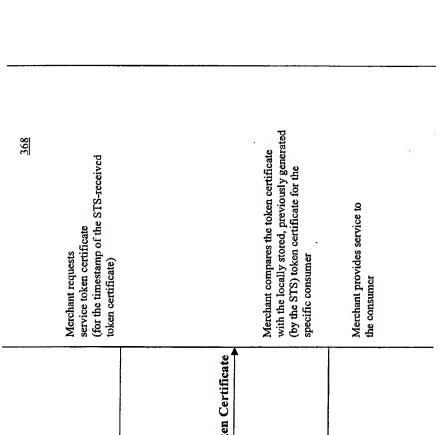


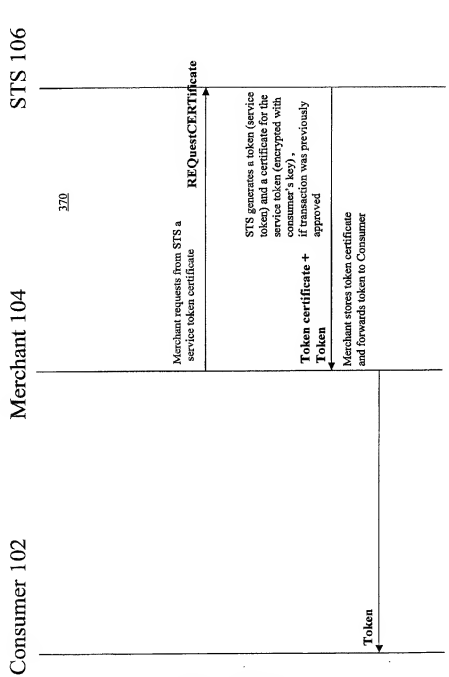
Figure 21

Single step REQuest, AUTHorization and Token Creation



Service Token Verification and Consumption

Figure 22



Token Creation

Figure 23

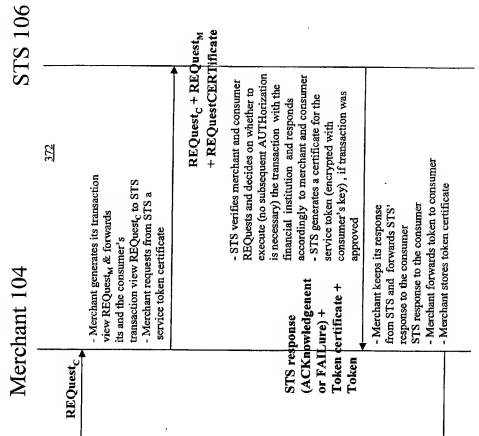
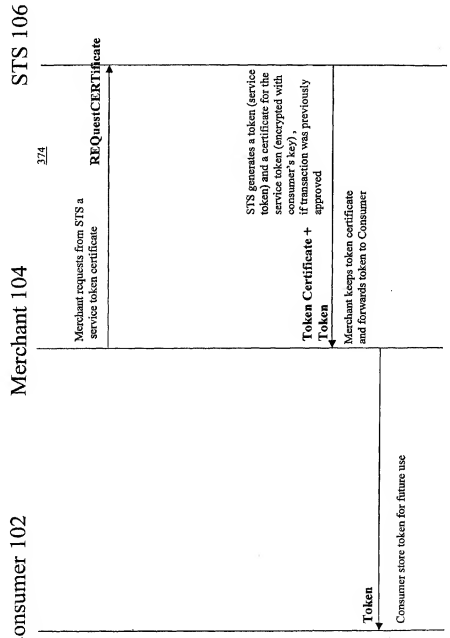


Figure 24

Single step REQuest, AUTHorization and Token Creation
(for token certificate verification by STS)



Token Creation
(for token certificate verification by STS)

Figure 25

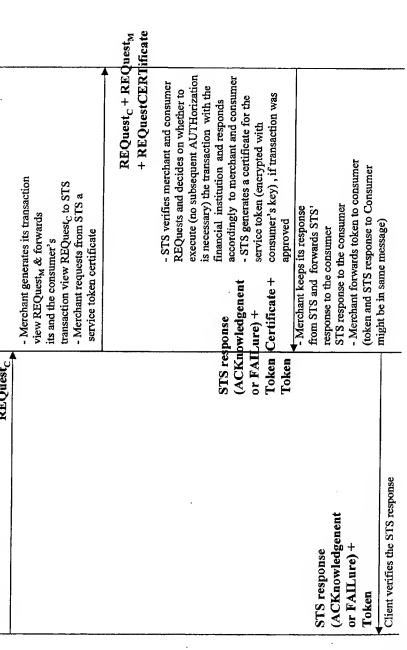
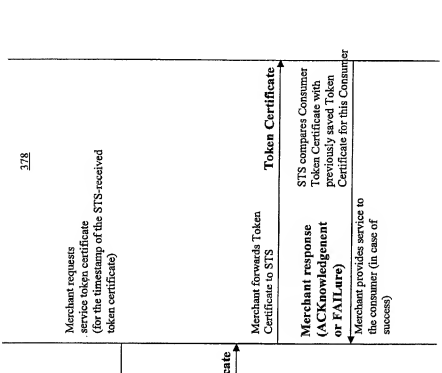


Figure 26

Single step REQuest, AUTHorization and Token Creation (for token certificate verification by STS)



Service Token Consumption (Verification by STS)

Figure 27

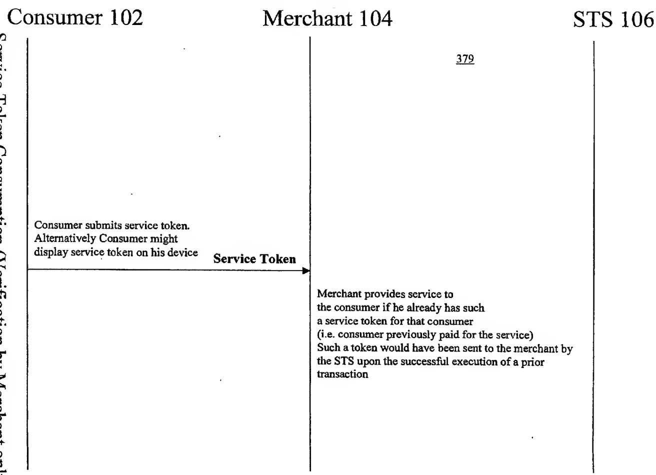


Figure 28

Service Token Consumption (Verification by Merchant only)

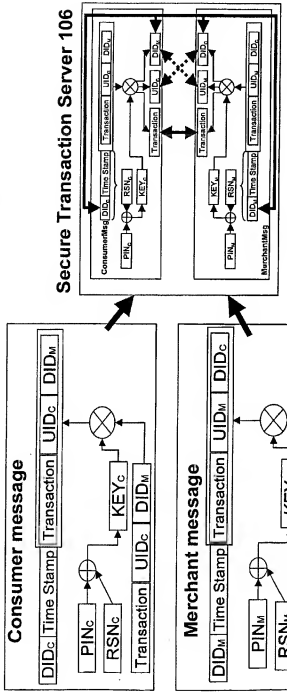

380
Secure Transaction Server 106
Consumer message
DIDc
Time Stamp
Transaction
UIDc
DIDM
PINc
RSNc
KEYc
Merchant message
DIDM
Time Stamp
Transaction
UIDM
DIDc
PINM
RSNM
KEYM
ConsumerMsg
MerchantMsg

Figure 29

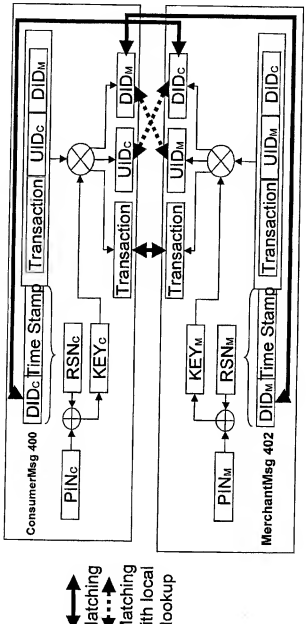

106
ConsumerMsg 400
DIDC
Time Stamp
Transaction
UIDC
DIDM
PINC
RSNC
KEYC
Transaction
UIDC
DIDM
Transaction
UIDM
DIDC
KEYM
RSNM
PINM
MerchantMsg 402
DIDM
Time Stamp
Transaction
UIDM
DIDC
Matching
Matching with local lookup

Figure 30

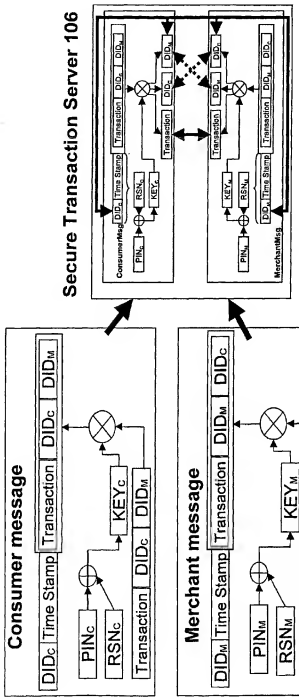

Consumer message
DIDc
Time Stamp
Transaction
DIDc
DIDM
PINc
RSNc
KEYc
Transaction
DIDc
DIDM
Merchant message
DIDM
Time Stamp
Transaction
DIDM
DIDc
PINM
RSNM
KEYM
Transaction
DIDM
DIDc
Secure Transaction Server 106
ConsumerMsg
DIDc
Time Stamp
Transaction
DIDc
DIDM
PINc
RSNc
KEYc
Transaction
DIDc
DIDM
Transaction
DIDc
DIDM
KEYM
PINM
RSNM
DIDM
Time Stamp
Transaction
DIDM
DIDc
MerchantMsg

Figure 31

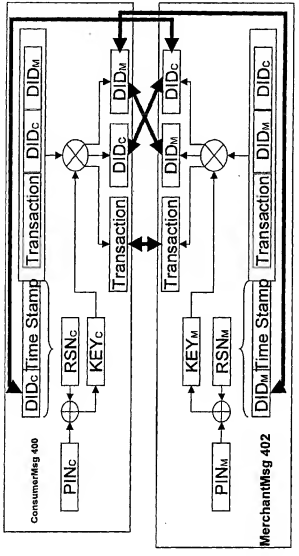

106
ConsumerMsg 400
DIDC Time Stamp
Transaction
DIDC
DIDM
PINC
RSNC
KEYC
Transaction
DIDC
DIDM
Transaction
DIDM
DIDC
KEYM
RSNM
PINM
MerchantMsg 402
DIDM Time Stamp
Transaction
DIDM
DIDC
Matching

Figure 32

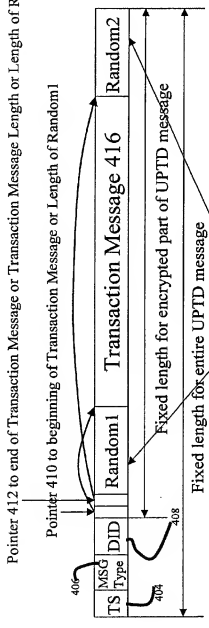
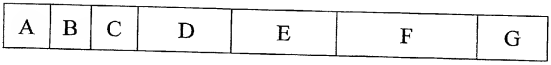

Pointer 412 to end of Transaction Message or Transaction Message Length or Length of Random2
Pointer 410 to beginning of Transaction Message or Length of Random1
406
TS
MSG Type
DID
Random1
Transaction Message 416
Random2
404
408
Fixed length for encrypted part of UPTD message
Fixed length for entire UPTD message
400
Length of each "Random" section is random and decided at the time of message composition.
414: Random 1
418: Random 2

Figure 33

420



A: Message type (REQuest or AUTHorization; REQuest in this case)

B: Success Code for response to this message

C: Failure Code for response to this message

D: DID of message sending device

E: DID of other transacting party's device

F: Transaction amount or some other agreed transaction description

G: Friendly name of account to be used to pay D's user, amount E

F is optional and might be specified in AUTHorization message

Figure 34

422

A: Message type (REQuest or AUTHorization; REQuest in this case)

B: Success Code for response to this message

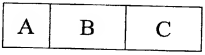
C: Failure Code for response to this message

D: DID of message sending device

E: DID of other transacting party's device

F: Transaction amount or some other agreed transaction description

Figure 35



A: The Success or Failure code indicated by Payer depending on whether the REQuest was successful or not

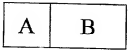
B: A randomly generated number to be used to refer to the transaction for the remainder of the change

C: Payer's account listing

Figure 36

EP 1 388 797 A2

426



A: The Success or Failure code indicated by Payer depending on whether the REQuest was successful or not

B: A randomly generated number to be used to refer to the transaction for the remainder of the exchange

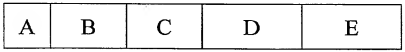
Figure 37

428

A: Message type (REQuest or AUTHorization; AUTHorization in this case)
B: Success Code for response to this message
C: Failure Code for response to this message
D: A reference to the transaction been authorized; a previously STS-generated reference is used
E: Optional to reference payer's account if not previously specified

Figure 38

430

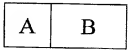


92

A: Message type (REQuest or AUTHorization; AUTHorization in this case)
B: Success Code for response to this message
C: Failure Code for response to this message
D: A reference to the transaction been authorized; a previously STS-generated reference is used
E: Optional to reference payee's account if not previously specified

Figure 39

432



A: The Success or Failure code indicated by Payer depending on whether the Authorization was successful or not

B: An optional additional description, for example a service token value (receipt)

Figure 40

434

A	B

A: The Success or Failure code indicated by Payee depending on whether the Authorization was successful or not

B: An optional additional description, for example a service token value (receipt)

Figure 41

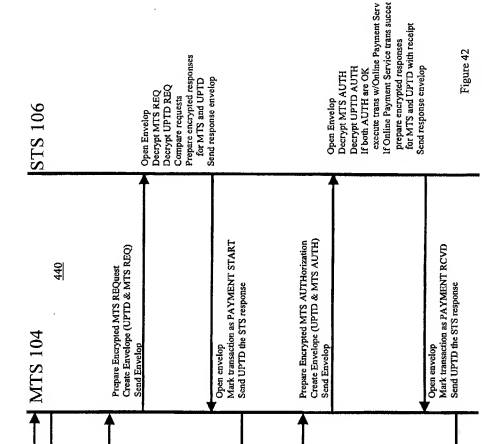

UPTD 102
Request PO
Send PO
Show PO to user
Request PIN
Prepare UPTD Encrypted REQuest
Send UPTD Encrypted REQ
Show response to user and store receipt
MTS 104
440
Decrypt message from STS
If REQ was OK ask for user AUTH
Request AUTHorization from User
User Selects account AUTHorizes
Send UPTD Encrypted AUTHorization
Prepare Encrypted MTS REQuest
Create Envelop (UPTD & MTS REQ)
Send Envelop
Open envelop
Mark transaction as PAYMENT START
Send UPTD the STS response
Prepare Encrypted MTS AUTHorization
Create Envelop (UPTD & MTS AUTH)
Send Envelop
Open envelop
Mark transaction as PAYMENT RCVD
Send UPTD the STS response
STS 106
Open Envelop
Decrypt MTS REQ
Decrypt UPTD REQ
Compare requests
Prepare account responses
for MTS and UPTD
Send response envelop
Open Envelop
Decrypt MTS AUTH
Decrypt UPTD AUTH
If both AUTH are OK
execute trans w/Online Payment Serv
If Online Payment Service trans succes
prepare response receipt
for MTS and UPTD with receipt
Send response envelop

Figure 42

1 Consumer Requests Purchase Order (PO)
2 Consumer Receives PO
3 Consumer REQuests transaction (consumer enters PIN)
4 MTS sends MTS REQ and consumer REQ
5 STS requests from Online Payment Service the account listing for consumer
6 STS receives Online Payment Service account listing
7 STS Sends response to REQ with accounts for consumer
8 MTS forwards STS response to REQ to consumer
9 Consumer AUTHorizes transaction (consumer selects account)
10 MTS sends MTS AUTH and consumer AUTH
11 STS sends transaction to Online Payment Service
12 STS receives Online Payment Service response
13 STS sends response to AUTH
14 MTS forward STS response to AUTH to consumer
(consumer sees notification of success on his display)

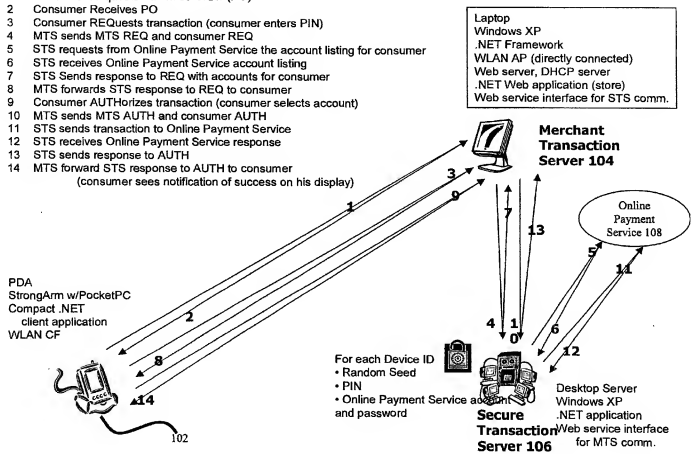


Figure 43

EP 1 388 797 A2

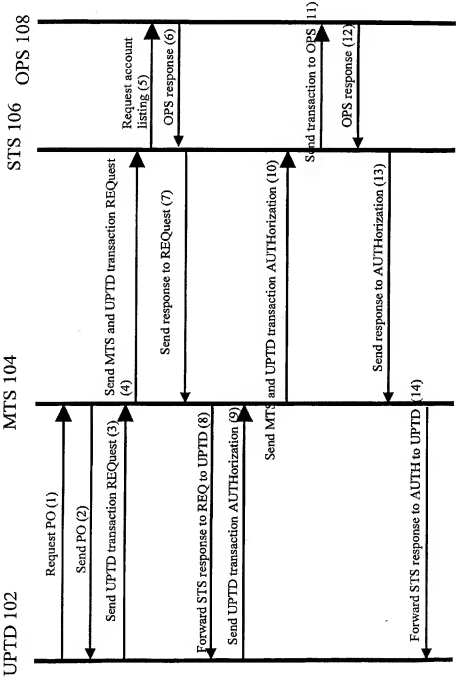

UPTD 102
MTS 104
STS 106
OPS 108
Request PO (1)
Send PO (2)
Send UPTD transaction REQuest (3)
Send MTS and UPTD transaction REQuest (4)
Request account listing (5)
OPS response (6)
Send response to REQuest (7)
Forward STS response to REQ to UPTD (8)
Send UPTD transaction AUTHorization (9)
Send MTS and UPTD transaction AUTHorization (10)
Send transaction to OPS (11)
OPS response (12)
Send response to AUTHorization (13)
Forward STS response to AUTH to UPTD (14)

Figure 44

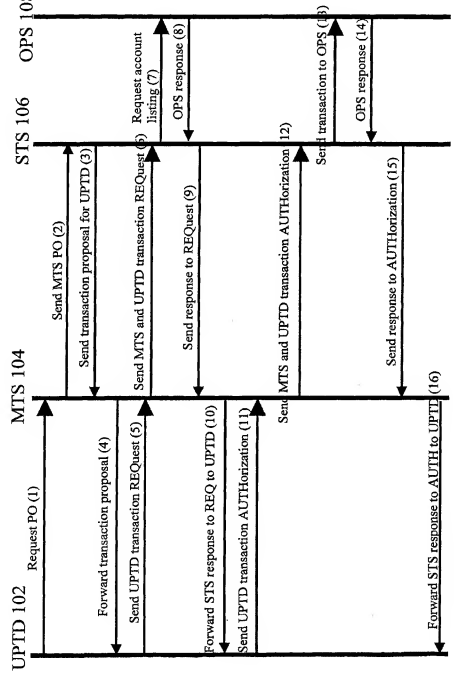

UPTD 102
MTS 104
STS 106
OPS 108
Request PO (1)
Send MTS PO (2)
Send transaction proposal for UPTD (3)
Forward transaction proposal (4)
Send UPTD transaction REQuest (5)
Send MTS and UPTD transaction REQuest (6)
Request account listing (7)
OPS response (8)
Send response to REQuest (9)
Forward STS response to REQ to UPTD (10)
Send UPTD transaction AUTHorization (11)
Send MTS and UPTD transaction AUTHorization (12)
Send transaction to OPS (13)
OPS response (14)
Send response to AUTHorization (15)
Forward STS response to AUTH to UPTD (16)

Figure 45

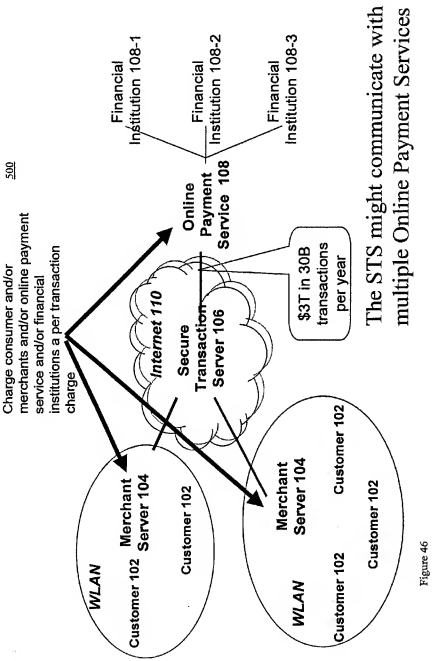

500
Charge consumer and/or merchants and/or online payment service and/or financial institutions a per transaction charge
WLAN
Customer 102
Merchant Server 104
Customer 102
Internet 110
Secure Transaction Server 106
Online Payment Service 108
Financial Institution 108-1
Financial Institution 108-2
Financial Institution 108-3
$3T in 30B transactions per year
WLAN
Customer 102
Merchant Server 104
Customer 102
Customer 102
The STS might communicate with multiple Online Payment Services

Figure 46

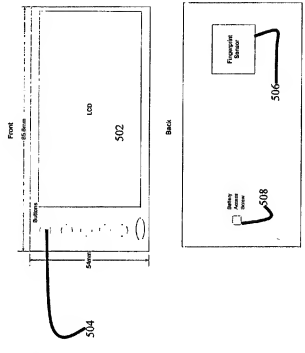

Front
LED Area
Buttons
Screen
LCD
502
Back
Fingerprint Sensor
506
Battery Release Button
508
102
504

Figure 47

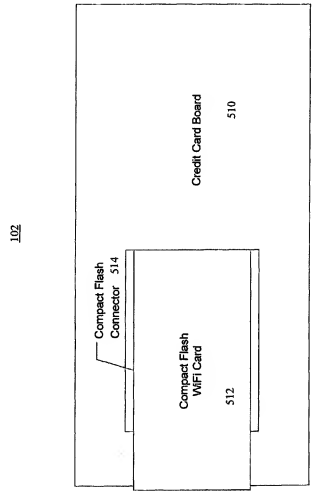

102
Compact Flash Connector 514
Compact Flash WiFi Card
512
Credit Card Board
510

Figure 48

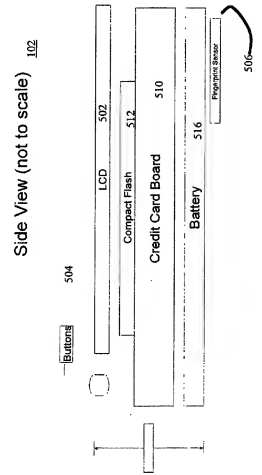

Side View (not to scale) 102
Buttons
504
LCD
502
Compact Flash
512
Credit Card Board
510
Battery
516
Proximity Sensor
506

Figure 49

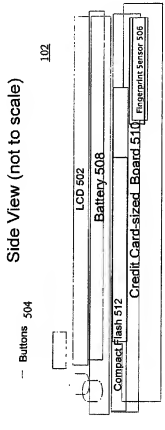

Side View (not to scale)
102
Buttons 504
LCD 502
Battery 508
Compact Flash 512
Credit Card-sized Board 510
Fingerprint Sensor 506

Figure 50

Pre-purchasing phase, example 600

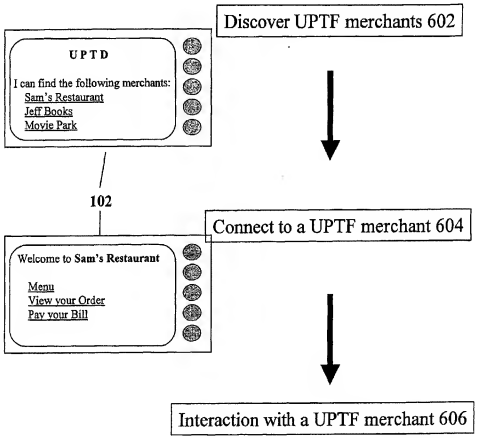


Figure 51

Physical Goods Purchase I, example 610

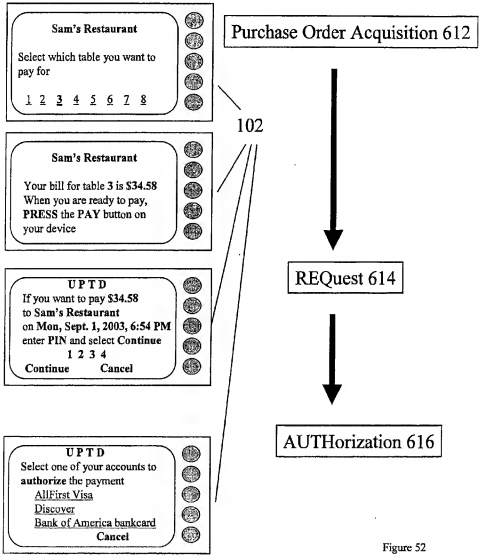


Figure 52

Physical Goods Purchase I, example, variation 620

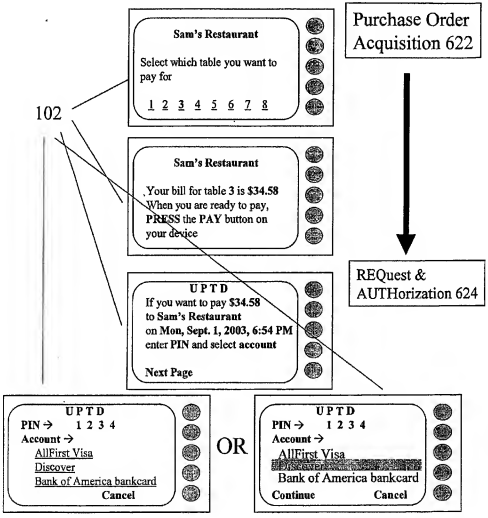


Figure 53

Physical Goods Purchase II, example 630

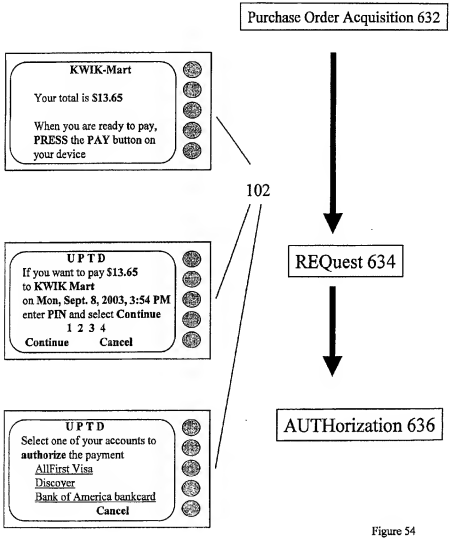


Figure 54

Service Purchase I, example 638

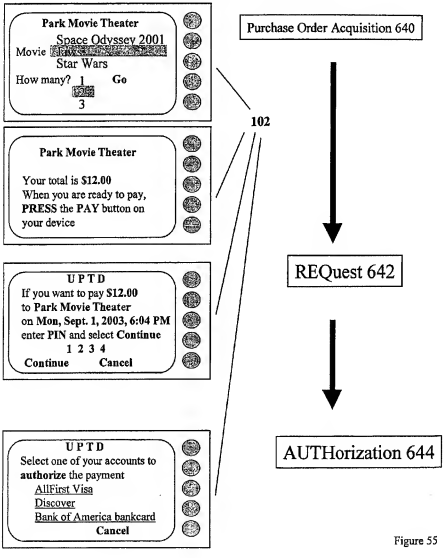


Figure 55

Service Purchase I – token verification and consumption, example 650

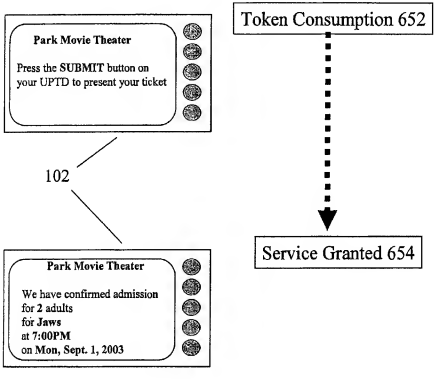


Figure 56

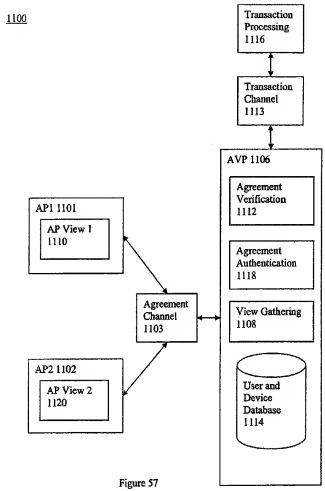

1100
Transaction Processing 1116
Transaction Channel 1113
AVP 1106
Agreement Verification 1112
Agreement Authentication 1118
View Gathering 1108
User and Device Database 1114
AP1 1101
AP View 1 1110
AP2 1102
AP View 2 1120
Agreement Channel 1103

Figure 57

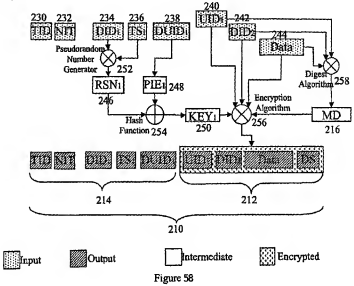

200
230
TID
232
NT
234
DIDi
236
TSi
238
DUIDi
240
UIDi
242
DIDj
244
Data
Pseudorandom Number Generator
252
RSNi
246
PIEi
248
Digest Algorithm
258
Encryption Algorithm
256
Hash Function
254
KEYi
250
MD
216
TID
NT
DID
TS
DUID
UID
DTM
Data
DS
214
212
210
Input
Output
Intermediate
Encrypted

Figure 58

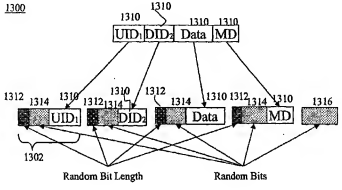

1300
1310
1310
1310
1310
1310
UID1
DID2
Data
MD
1312
1314
1310
1310
1312
1314
1310
1312
1314
1310
1316
UID1
DID2
Data
MD
1302
Random Bit Length
Random Bits

Figure 59

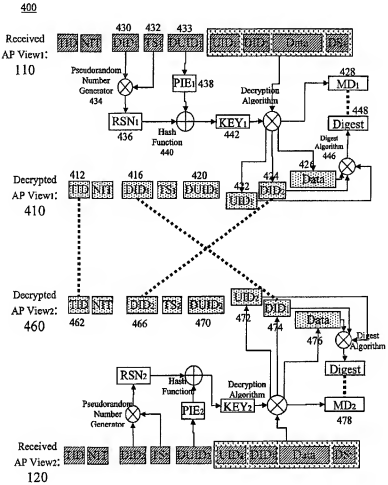

400
Received AP View1: 110
TID
NTI
DID1
TS
DUID1
UID2
DID1
Data
DS1
Pseudorandom Number Generator 434
PIE1 438
Decryption Algorithm
MD1 428
Digest 448
RSN1 436
Hash Function 440
KEY1 442
Digest Algorithm 446
Data 426
Decrypted AP View1: 410
412
416
420
422
424
DID2
UID1
Decrypted AP View2: 460
462
466
470
472
474
476
DS2
RSN2
Hash Function
Pseudorandom Number Generator
PIE2
KEY2
MD2 478
Received AP View2: 120

Figure 60

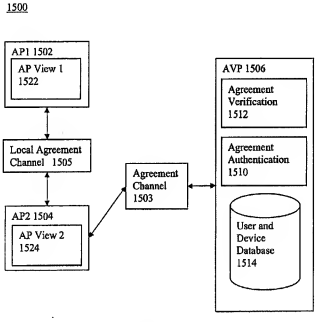

1500
AP1 1502
AP View 1
1522
Local Agreement
Channel 1505
AP2 1504
AP View 2
1524
Agreement
Channel
1503
AVP 1506
Agreement
Verification
1512
Agreement
Authentication
1510
User and
Device
Database
1514

Figure 61

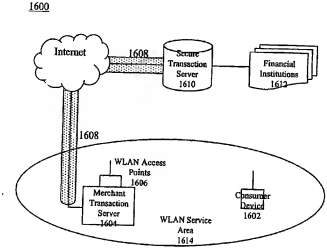

1600
Internet
1608
Secure Transaction Server 1610
Financial Institutions 1612
1608
WLAN Access Points 1606
Merchant Transaction Server 1604
WLAN Service Area 1614
Consumer Device 1602

Figure 62

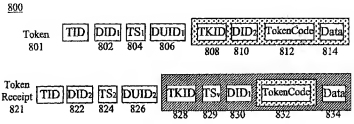

800
Token
801
TID
DID1
802
TS1
804
DUID1
806
TKID2
808
DID2
810
TokenCode
812
Data
814
Token
Receipt
821
TID
DID2
822
TS2
824
DUID2
826
TKID2
828
TS2
829
DID1
830
TokenCode
832
Data
834

Figure 63